AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

OBSCENE MATERIAL AVAILABLE VIA THE INTERNET

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MAY 23, 2000

Serial No. 106–115

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
64–763CC WASHINGTON : 2000

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
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
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *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
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ROBERT L. EHRLICH, Jr., Maryland
TOM BLILEY, Virginia,
(Ex Officio)

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

CONTENTS

	Page
Testimony of:	
Burgin, Joseph W., Jr	31
Flores, J. Robert, Vice President and Senior Counsel, National Law Center for Children and Families	13
Laaser, Mark R., Executive Director and Cofounder, Christian Alliance for Sexual Recovery	7
LaRue, Janet M., Senior Director of Legal Studies, Family Research Council	26
Gershel, Alan, Deputy Assistant Attorney General, Criminal Division; accompanied by Terry R. Lord, Chief, Child Exploitation and Obscenity Section, Criminal Division, Department of Justice	49
Stewart, Tracy R., Head of Technology, FamilyClick.com, LLC	18
Material submitted for the record by:	
Largent, Hon. Stene, a Representative in Congress from the State of Oklahoma, letter dated June 8, 2000, to Hon. W.J. "Billy" Tauzin, enclosing material for the record	77

(III)

OBSCENE MATERIAL AVAILABLE VIA THE INTERNET

TUESDAY, MAY 23, 2000

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

The subcommittee met, pursuant to notice, at 10:10 a.m., in room 2123, Rayburn House Office Building, Hon. W.J. "Billy" Tauzin (chairman) presiding.

Members present: Representatives Tauzin, Oxley, Stearns, Deal, Largent, Shimkus, Pickering, Ehrlich, Bliley (ex officio), Luther, and Green.

Staff present: Linda Bloss-Baum, majority counsel; Mike O'Reilly, professional staff; Cliff Riccio, legislative assistant; and Andy Levin, minority counsel.

Mr. TAUZIN. The subcommittee will please come to order.

Today the subcommittee convenes to discuss the perplexing subject of obscenity and sexually explicit material available on the Internet. I say that it is perplexing because while the law governing obscenity has been well established for years, many pornographers and others that broadcast sexually explicit material today online seem to be immune from prosecution under applicable Federal law.

In fact, an example of the apparent Justice Department reluctance in this matter was exhibited just this morning. The Attorney General's office at the Department of Justice was here today to testify, and they exercised their discretion in leaving this committee room and refusing to testify because we made a simple request that they sit and listen to the witnesses first and comment on their testimony. They claim the Department of Justice will not sit and listen to constituents at a hearing, and so they have taken upon themselves to leave this hearing room and have refused to testify in the order in which the Chair has set the testimony.I find this absolutely a great example of the arrogance of our current Justice Department.

Let my say it again: They wouldn't sit and listen to the witnesses who want to complain about the fact that the Justice Department has refused or somehow been totally negligent in enforcing the obscenity laws of this country.

So we will not hear from the Justice Department this morning, but you can rest assured that the Attorney General will be hearing from this committee in regards to the performance of her witnesses

this morning who have, as I said, chosen to leave this hearing room rather than testify following the testimony of the witnesses who are gathered to discuss this important subject with us today.

Not even the Supreme Court has denied that sexually explicit material exists on the Internet. Material extends from modestly titillating to the hardest core material you can imagine. Disturbing enough, a great deal of this material is in fact legally obscene under the so-called 3-point Miller test established by the Supreme Court because it appeals to prurient interests, is patently offensive and lacks any literary, artistic or political value in any community where viewing such material is possible. This material therefore is unprotected by the first amendment, which means that it can be regulated at all levels of government. Not surprisingly, both the Federal Government and every State that I know of have implemented obscenity laws that restrict the distribution of obscene material to varying degrees and ban child pornography altogether.

And with reference Title 18, Sections 1462, 65, 66, 67 and 1470, the Supreme Court stated in Reno versus ACLU, the very case which struck down challenged provisions of the communications act, the decency act, the CDA—this is a quote from the Supreme Court—"Transmitting obscenity, whether via the Internet or other means, is already illegal under Federal law for both adults and juveniles."

Despite that the main point of the decision in Reno versus ACLU was that the challenged provisions of the challenged decency act did not pass constitutional muster, the case is just as important for the Federal courts' observation of existing Federal obscenity law.

I quote from a U.S. District court's opinion which was upheld by the Supreme Court. "Vigorous enforcement of current obscenity and child pornography laws should suffice to address the problem the government identified in court and which concerned Congress when it enacted the CDA. When the CDA was under consideration by Congress, the Justice Department itself communicated its view that CDA was not necessary because it, Justice, was prosecuting online obscenity, child pornography and child solicitation under existing laws and would continue to do so."

Well, ladies and gentlemen, the point the court is making is very simple. Regardless of what happened to CDA, the laws already on the books are clear and strong, strong enough to control obscenity. Unfortunately, however, one does not get that impression when reviewing the DOJ's record of prosecuting purveyors of obscene material online under Federal law.

We are not here today to entertain or consider specific legislation. To the contrary, we are here to better understand why the Clinton administration refuses to enforce existing Federal obscenity laws against purveyors of this absolute filth that is accessible to just about every man, woman and child on the Internet. Frankly, I think the Justice Department's record in prosecuting online obscenity is an embarrassment, and I am not surprised that Justice Department witnesses walked out of this hearing room today, and I find it appalling that despite the sufficiency of our laws, Justice has broken its promise to appropriately prosecute.

Under this administration it cannot be denied that we have witnessed the most explosive growth in distribution of obscenity to all

ages in American history, hardly the result we intended when we amended Title 18.

So today I look forward to getting to the bottom of this quagmire. We certainly hoped that the Department of Justice was ready to talk to us and answer questions after they had heard the presentation of our witnesses. That hope was apparently misplaced this morning as the Justice Department has decided to walk out of this hearing.

The Chair will yield to the gentleman from Ohio for an opening statement.

Mr. SAWYER. Thank you, Mr. Chairman. I suspect that there is another side to the story in terms of why the Justice Department chose not to be here, and I don't take issue with anything that you have said, particularly in terms of raising questions about what that motivation might be.

Mr. TAUZIN. Would the gentleman yield?

Mr. SAWYER. I prefer just to continue if I could. I don't take issue—I don't question what you are saying, only to suggest that there is, I would suspect, another side to the story.

Mr. TAUZIN. Would the gentleman yield?

Mr. SAWYER. I would be happy to.

Mr. TAUZIN. I will extend the gentleman time. I simply want to point out, if there is another side we didn't hear it this morning. The Justice Department's only objection was that they didn't want to sit and listen——

Mr. SAWYER. Reclaiming my time, I am as frustrated as you are that they didn't stay to make that point clear, but I suspect that there is another side to that story, and I hope that people who are interested will pursue that as I can assure you I will and I hope you will do as well, Mr. Chairman.

My frustration is, as you suggest, that there is strong and powerful law with regard to the enforcement of existing statutes against pornography and indecency, and the medium through which that is transmitted ought not to make a substantial difference. It is particularly true at a time when we see media merging, where the kind of findings that we are seeing through the courts with regard to television will increasingly apply to similar kinds of depiction on the Internet.

As we see these media merge, as we have already seen on a basic level, we come back to questions that we have reviewed in other contexts: Should the Internet be treated any differently? Would it be wise to regulate TV in one way and the Internet in another? Are current filters really feasible? Are they effective? If they are not, what can be done? What Federal regulations can be effective if technologies are not available? How can we apply the Miller test using contemporary community standards when the community that we are talking about, particularly with regard to the Internet, is virtually global in its scope?

There are serious questions, Mr. Chairman. I am pleased that you have called this hearing. I am frustrated that we will not hear from everyone today, but having said that, I would hope that there would be an opportunity for an additional hearing at which the Department of Justice might have a chance to testify.

Mr. TAUZIN. Will the gentleman yield?

Mr. SAWYER. Yes.

Mr. TAUZIN. Apparently the Department of Justice witnesses have just informed the subcommittee that they are now prepared to visit with us after the first panel. So apparently we will hear from them now.

Mr. SAWYER. Good. I am as comforted by that as I suspect you are.

Mr. TAUZIN. I am very comforted.

Mr. SAWYER. With that, Mr. Chairman, let me just say that this is not only a matter of standards and values, this is a question of technical feasibility and a question in this digital environment of what we mean by community standards when that community is as large as all of humanity.

Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman. I point out, however, that they have left the room. Apparently they may or may not be here when the first panel discusses the issue. I would hope that they return, at least sit and hear from citizens of this country who are concerned about the matter. But we will see how that progresses.

The Chair is now pleased to welcome the chairman of the full committee, the gentleman from Richmond, Virginia, Mr. Bliley.

Chairman BLILEY. Thank you, Mr. Chairman, for holding this hearing. I would also like to thank our friend Steve Largent for his work on the issue of obscene material that is being made available via the Internet. He should be commended for his due diligence.

People who make obscene material and child pornography available on the Internet should be investigated and prosecuted to the fullest extent of the law. Frankly, I do not feel that the Justice Department has done enough in this area. The fact remains that people are breaking the law every day. Obscene material and child pornography have always been against the law. Through the Communications Decency Act, we made it illegal on the Internet as well, but there needs to be a cop on the beat to keep things secure and to protect society from the deviants who sell, show or promote this type of material.

This is the job of the Justice Department, and I do hope that they do come back and testify today. I think it is shameful that they would not listen to citizens and to hear their complaints. We see that too often in Federal agencies that they go their own way and they are not interested in listening to the people who they are supposed to be looking out for, and that is a shame.

Congress established the COPA commission to come up with ideas that help parents protect their kids from indecent material on the Web. I look forward to completion of the work of the commission. I am hopeful that their recommendations to Congress will provide further insight on how to help cut down on the exposure to the material we are discussing today.

I want to thank the witnesses for coming today. It is important to help the many folks who have fallen prey to the massive amounts of obscene material available over the Internet. This whole discussion, Mr. Chairman, sort of reminds me back in the early eighties when we were trying to stamp out the Dial a Porn, if you remember, and what a time we had. You would think that common sense would prevail, but it took us about 5 or 6 years be-

fore we could get a handle on it. I hope it doesn't take that long this time.

Thank you.

Mr. TAUZIN. I thank the gentleman.

The Chair is now pleased to welcome the gentleman from Oklahoma, Mr. Largent, with the Chair's thanks for his extraordinary diligence in pursuing this matter with the committee, and Mr. Largent is recognized.

Mr. LARGENT. Thank you, Mr. Chairman, for holding this hearing. I think it is a very important hearing and I am glad that this subcommittee has the opportunity, hopefully will have the opportunity to discuss with the Department of Justice their efforts to prosecute Internet obscenity.

Publications for the adult industry have been puzzled over how likely it is that the adult entertainment industry will enjoy the same, and I quote, "benevolent neglect" under the next administration that the industry has enjoyed under Janet Reno. It is my understanding that there have been no prosecutions of Internet obscenity by the Department, and I am eager to hear from our Department of Justice witness on this issue.

I am deeply concerned with the type of easily available obscene content on the Internet today. By definition, obscenity is patently offensive, appeals to the prurient interest in sex and has no serious literary, artistic, political or scientific value. It is illegal to distribute to any person including adults, and yet the level of filth and vile on the Internet is inconceivable, with estimates for the number of adult Web sites ranging from 40,000 to over 100,000 or more.

The amount of material on the Net is growing exponentially and nobody is quite sure how many sites exist. Such material would never be allowed in a bookstore or on television. Do we think the social costs and community problems previously associated with adult bookstores and hard core strip clubs have diminished because it is on the Internet? Certainly not. Instead they have become more prevalent, more internalized and more destructive.

The aggressive marketing tactics of the adult industry have brought such material directly into the family rooms of millions of Americans and also into our schools' libraries and into the schools themselves. By such aggressive tactics as spam e-mail, page-jacking and mouse-trapping, innocent adults and children are lured into a world they did not wish to see and from which it is difficult to escape once online.

Furthermore, the lack of prosecution has given a false sense of legitimacy to this industry. Revenues generated by pornography exceed the revenues generated by rock and country music combined. Adult entertainment sites on the Internet account for the third largest sector of sales in cyberspace, only behind computer products and travel, with an estimated $1-$2 billion per year in revenue.

I would ask the committee to remember the following facts. Obscenity is illegal under Federal law. Obscenity has been defined by the Supreme Court. Obscenity is not protected by the first amendment. It degrades women and diminishes a child's ability to conceive of a healthy view of adult relationships. It is a destructive force which is polluting the minds of adults and children alike. We must aggressively prosecute obscenity in order to uphold the law,

protect all Americans from such illegal material and especially protect our children from such material.

Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman.

The Chair will call the panel forward, please. I am sorry; Mr. Shimkus has arrived, the gentleman from Illinois.

Mr. SHIMKUS. Thank you, Mr. Chairman. I just applaud the work of my colleague, Mr. Largent, and look forward to the panel discussion. I yield back my time.

Mr. TAUZIN. I thank the gentleman.

[Additional statement submitted for the record follows:]

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

Thank you, Mr. Chairman. I believe this is a serious matter, and I'm glad the Subcommittee is reviewing it.

Let me say up front that I believe some agencies, the FBI and the Customs Service in particular, are doing excellent and very important work in this area. These agencies are staffed by law enforcement professionals who take stalking, abduction, and child pornography cases very, very seriously.

I also want to praise the Department of Justice for its vigorous defense of the Child Online Protection Act. We are currently awaiting a ruling from the Third Circuit, although I must say yesterday's deeply disappointing Supreme Court decision regarding unscrambled sexually explicit cable programming would not appear to bode well. The issues in the two cases are not the same, but I must say that I'm perplexed that five Justices would vote to strike those rather modest provisions of the Telecom Act.

What the ruling shows, I think, is that for the time being we-may need to rely on existing law to protect American families from the corrosive effects of hardcore pornography. Fortunately, existing law is rather strong, and as Presidents Reagan and Bush demonstrated, can be used to great effect in the fight against hardcore porn.

Unfortunately, the present administration has utterly abandoned the war against obscenity. In this area, there is nothing remotely resembling leadership coming from the White House or the Vice President's mansion.

For anyone who doubts this, let's look at some recent facts: In 1997, U.S. Attorneys prosecuted only 6 obscenity cases. In 1998, there were 8 prosecutions. In 1999, as near as I can tell, there were none. The level of federal obscenity enforcement dropped more than 80% during the first six years of the Clinton administration. *Adult Video News*, apparently the trade publication of the porn industry, actually endorsed Bill Clinton for re-election in 1996.

Also from *Adult Video News,* in an article entitled "A Ridiculous Amount of New Adult Product," comes this tidbit: 5,775 new adult releases hit the market in 1995, marking a staggering 80% increase from the year before. In 1996, there were 7,800 new hardcore video releases.

Contrast this with some of the reports during the Reagan and Bush years. Here's a quote from a 1986 New York Times article entitled "X-Rated Industry in a Slump:" "The pornographic industry's plight is due partly to legal challenges . . . with a little help from the Reagan administration, an unlikely alliance of conservatives and feminists has persuaded many retailers to stop carrying adult magazines and videos . . . Said Martin Turkel, one of the largest distributors of adult videos in the country, 'Next year is going to be the roughest year in the history of the industry.'"

And from Billboard: sales of adult videos at the wholesale level dropped from $450 million in 1986 to $386 million in 1987. That's compared to $3.9 BILLION in 1996.

And to sort of sum it up, here's a quote from a Los Angeles Daily News article about one year into President Clinton's first term: "Before Clinton took office, Los Angeles police were deputized by the federal government so they could help prosecutors conduct monthly raids on Valley pornographers. Under Clinton, there have been no raids," said Los Angeles police Lt. Ken Seibert. Seibert said, "Adult obscenity enforcement by the federal government is practically nonexistent since the administration changed."

Even more than new laws, Mr. Chairman, we need more enforcement of existing obscenity statutes. I yield back.

Mr. TAUZIN. Will the witnesses please step forward? They include Mr. Mark Laaser, the executive director and cofounder of the Christian Alliance for Sexual Recovery; Mr. Robert Flores, vice president and senior counsel of the National Law Center for Children and Families; Ms. Tracy Stewart, the head of technology at FamilyClick.com; Ms. Jan LaRue, senior director of legal studies for the Family Research Counsel here in Washington, D.C.; Mr. Joseph Burgin of Cincinnati, Ohio. And we had Ms. Kathie LeRose on the agenda today, and apparently she lost a family member, her father, so we want to keep her in our thoughts today. She is not able to attend. Apparently her father suffered a heart attack today.

So we want to welcome our panel, and under the rules panelists are reminded that we have a timing system. You should look at these devices in front of you. They accord you 5 minutes to summarize your statements, hit the keep points for us.

Your written statements are already a part of our record. By unanimous consent, without objection, all written statements of members and panelists are made a part of our record. So ordered, and we will ask you, as I call you forward, to summarize within 5 minutes so that we can get to Q and A as rapidly as we can.

We will start with Mr. Mark Laaser, the executive director and cofounder for the Christian Alliance for Sexual Recovery. Mr. Laaser.

STATEMENTS OF MARK R. LAASER, EXECUTIVE DIRECTOR AND COFOUNDER, CHRISTIAN ALLIANCE FOR SEXUAL RECOVERY; J. ROBERT FLORES, VICE PRESIDENT AND SENIOR COUNSEL, NATIONAL LAW CENTER FOR CHILDREN AND FAMILIES; TRACY R. STEWART, HEAD OF TECHNOLOGY, FamilyClick.com, LLC; JANET M. LaRUE, SENIOR DIRECTOR OF LEGAL STUDIES, FAMILY RESEARCH COUNCIL; AND JOSEPH W. BURGIN, JR.

Mr. LAASER. Thank you, Mr. Chairman, and thank you honorable members of this committee. You have my written testimony in front of you, and it summarizes some key points as I was able to ascertain them from the existing research in the field of the damaging effects of obscene material available on the Internet. I would direct you to the summary statement and I will just briefly go over that at this time.

Research has shown that 60 percent of all Web site visits access sexually related sites containing obscene material. It is estimated and one research study has in fact confirmed that 60 percent of all——

Mr. TAUZIN. Let me explain, those bells are advising Members of votes on the House floor. This is going to happen during our hearing process. This in effect is saying we have a 15-minute vote followed by two 5-minute votes which will take us away for about a half hour. So we will go on for about 10 more minutes and then we will recess for about a half hour and come back. Mr. Laaser.

Mr. LAASER. I was just saying that it is estimated that 60 percent of all male computer time at work is dedicated to accessing pornography, and of course, as most of us are aware and as you said, the growth of the Internet is exponential. It is estimated that by the year 2001, 95 million Americans will have online access.

I should say before I continue that I am here today in my role as an expert in the field of Internet pornography, and one of the reasons I got into the field was because prior to the development of the Internet, I was myself addicted to pornography for 25 years of my life. It would be unfair for me not to say that I obviously have some biases because I am myself a person who was lost in this world, and I thank God that the Internet was not available to me, because if it had been, I would certainly have been farther down the road than I was.

The major thing that concerns I think all of us is the growth of child pornography that is available. As you will see in my written testimony, even the United States Department of Commerce has recognized that the growth of child pornography is a major threat to the welfare of children.

Pornography that is violent in nature is certainly available in a variety of forms. The other day in preparing for my testimony, I pulled up a menu that included 25 forms of sadomasochistic activity, including bloodletting, so that we know that violent pornography exists, and I got into it in less than 60 seconds.

Pornography has the ability, according to all psychological theory, to program children early. We are now seeing research that is telling us that whereas in my generation of men, the average age a person first saw pornography was age 11, now it is age 5. A child who has the ability, and we are teaching them in school to do this, can get into these sites very easily; 4-, 5-, 6-, 7-year-olds now are seeing things that in my extensive history with pornography I never saw, pornography that is being seen as violent, it is degrading, it humiliates people and is teaching our children very immature, immoral and damaging roles about themselves.

All psychological theory would certainly confirm that this kind of material, even if it is in its softest form, has the ability to affect a child's attitude, sexual orientation and sexual preferences for the rest of their life.

Internet pornography also can become very addictive. Addiction is progressive and leads to more destructive forms of sexual acting out later in life. All of us who work in this field have seen tremendous social, legal, vocational, financial and physical consequences as a result.

I would point you to a case study that I put in my written testimony of a family that I have been treating. The 8-year-old daughter was doing a research project on Cinderella, put in the word "Cinderella" to a search engine. The Web site that came up to her was the picture of a woman who was named Cinderella but was using an artificial penis to self-stimulate herself. So this 8-year-old girl, who had been doing what the parents considered to be healthy research, was immediately exposed to very harmful and violent material.

I would also tell you that our anecdotal experience would suggest now that women are being exposed to pornography in greater and greater numbers and rates. Women are now becoming equally addicted to forms of pornography on the Internet. We are seeing an epidemic rise in the number of cases that we are treating. The belief is in the psychological community that every person has the ability to be hard wired and to be programmed into various kinds

of sexual preference. I believe that we are literally changing the way women view sexuality in themselves.

In the third section of my written testimony I describe what I believe is one of the unique problems with the availability of the Internet, in that we call it the triple engine, and that is, that it is accessible. It used to be that when I was addicted to pornography you had to go to some far-off bookstore. Now today you it can do it in your own home. It is affordable. A lot of the Web sites offer loss leaders and free material, and it is certainly anonymous, so that many of the prohibitions that may have stopped people historically are not present.

But I think No. 2 here in my summation, the thing that concerns me the most is the accidental nature that even adults or children who are accessing the Internet for healthy purposes will be bombarded and barraged. And I would say, Mr. Chairman, that all of us in the field would consider that the accidental nature of Web sites that can come up, pictures that can come up, e-mails that can come up, is a form of sexual assault that is not being regulated in this country and I would emphasize the word "sexual assault." We would get very upset if we knew that any of our children were being sexually assaulted in any way.

That would conclude my summation. I will leave you to read any recommendations which may or may not be relevant to this committee.

[The prepared statement of Mark R. Laaser follows:]

PREPARED STATEMENT OF MARK R. LAASER, DIRECTOR, CHRISTIAN ALLIANCE FOR SEXUAL RECOVERY

Mr. Chairman and honorable members of the Commerce Committee: It is my honor to be able to testify before this committee. The issues of pornography and of violence on the Internet are vitally serious ones. The damaging effects on millions of lives is profound.

My background is that I am trained as a Christian minister and a doctoral level counselor. I have authored several books in the area of sexual addiction, sexual compulsivity, and sexual abuse. Perhaps more importantly, I have been in recovery from a sexual addiction to pornography and other forms of sexual acting out for thirteen years. My own life is an example of how damaging the effects of pornography can be. Thankfully, my "sobriety" which started in 1987 precedes the availability of Internet pornography. My remarks based on the limited research that is available in the field and on my work with hundreds of men, women, and teenagers who have been effected by Internet pornography.

My remarks can be divided into three areas: 1. The Damaging Effects of Internet Pornography; 2. Unique Dangers Presented by the Internet; and 3. Suggestions For What Might Be Done.

THE DAMAGING EFFECTS OF INTERNET PORNOGRAPHY

Prevalence

Various research studies have demonstrated the escalating usage of sexually oriented sites on the Internet. In a 1998 study of hundreds of on-line users, Dr. Al Cooper found that 15% had accessed one of the top five sex web sites. A follow up study in 1999 reported that 31% of on-line users visited web sites dedicated to pornography. In the most recent study, the Sexual Recovery Institute of Los Angeles conducted a research survey and found that 25 million Americans visit cyber-sex sites every week and that 60% of all web site visits are sexual in nature. It is estimated that by next year 95 million Americans will have access to the Internet.

In the most recent issue of the journal *Sexual Addiction and Compulsivity* several authors contend that accessing sexually oriented web sites is not confined to the home but is a primary problem at work. One study by a leading Fortune 500 company found that 62% of male computer time was spent in cyber-sex sites. A friend of mine, who is a vice-president of one of our large Twin Cities based companies,

recently had to fire 20 top level executives because of uncontrolled pornography usage on company owned computers.

It is commonly accepted by all researchers that sexually oriented web sites are a tremendous growth industry around the world. Hundreds of new ones are added every week. Entering even remotely sexually related words into any search engine will result in thousands of sexually based web site possibilities.

In 1986, the Attorney General's Select Commission on Pornography sent a report to Congress. This report was unanimous in a number of findings: 1. It condemned all sexually explicit material that was violent in nature. 2. It condemned all sexually explicit material that depicted women in positions that are humiliating, demeaning, and subjugating. 3. It was opposed to child pornography in any form.

There is no debate that violent pornography proliferates on the Internet. In preparing for this testimony, for example, I pulled up a cyber-sex web site menu through my AOL search engine that contained listings for 25 different forms of S&M including blood letting. The forms of violent sexual deviance that can graphically be displayed are almost beyond description. Sadly, I am also aware through several of my clients that depiction of mutilization and death, so called "snuff" material is available.

Since the Attorney General's commission report, it is my opinion that all forms of pornography are degrading to whomever is being portrayed. It is not just women who can be portrayed in humiliating fashion. The growing number of females who are visiting sexually oriented web sites along with a heavy percentage of male homosexual usage has caused an increase in the amount of degrading pornography depicting men.

In the 1970s and 1980s, changes in pornography laws sharply reduced the availability of child pornography. The Internet, however, brought massive amounts of it back into the world. The U.S. Customs Service says on its current web site, "The presence of child pornography on the internet and on BBS services is a disturbing and growing phenomenon."

While there has been some success in regulating web sites devoted to child pornography, most of this kind of pornography is trafficked through bulletin board systems (BBS) with "picture files" that can be hidden in a variety of ways, and with Usenet News groups. These last use binary groups, digitized photographs, which can be transformed, in a variety of ways. This is not to mention the transmission of e-mails with photo attachments. While the most common depictions are of child nudity, children in erotic poses, and depictions of children in sexual activity, there is an incredible amount of depictions of rape, bondage, S&M, and adult-child intercourse.

Various forms of Damage

Specialists in the field of sexuality can be divided about sexual material available on the Internet. Some even suggest that it has educational value, decreases some unhealthy inhibitions, and is an otherwise unavailable social outlet. Few would disagree, however, that certain forms of pornography, as just described above, are universally damaging

Of chief concern should be possible damage to children. There can be little doubt for any of us parents that our children are more computer literate than we are. Even a five year old might have the computer skills to access any form of web site. Some have even suggested, as a result, that the average age a child first sees pornography has decreased from age 11 to age 5. We can't discount the other forms of pornography that are more readily available today than when I first say pornography in 1961.

According to the book *Protecting Your Child in Cyberspace* by Steve Kavanagh, a licensed mental health professional, "There are many studies that suggest that exposure to pornography can make kids act out sexually against other children . . . It seems clear that viewing deviant sexual behavior on the internet can cause a child to develop sexual deviance, which can shape sexual preferences that carry over into adulthood." In computer terms, a child's brain can be programmed neuro-anatomically for various forms of sexual orientation. While the brain can't manufacture new brain cells it continually manufactures connections between them.

Dr. John Money of Johns Hopkins University first described the theory that the brain is most critically programmed sexually during early childhood in his 1986 book Lovemaps. Dr. Money's groundbreaking work suggests that most forms of sexual deviance can be traced to experiences in childhood. Simply exposing a child to images of deviant sexual activity can have a profound effect. My own personal experience, and the experience of over a thousands clients would confirm this theory. I would emphasize that it is not just hard-core pornography that can have this effect.

Many psychologists, such as Dr. Judith Riesman, argue that even the so-called "softer" forms, such as in popular magazines, can be just as damaging.

Theories of sexual addiction and compulsivity are controversial in the clinical community. There is no doubt that the majority of on-line Internet users don't become addicted to the pornography that can be found there. There is also no doubt in my mind that many do. Some researchers are even starting to suggest that some who might not otherwise have become addicted to sex, are now doing so because of the Internet.

One of the stumbling blocks in the clinical debate about whether sex can be an addiction centers on the concept of chemical "tolerance." Many in the medical community feel that for substance or activity to be addictive it must create a chemical tolerance. Alcoholics know, for example, that over the lifetime of their addiction, they must consume more and more alcohol to achieve the same effect. New research, such as by Drs. Harvey Milkman and Stan Sunderwirth, has demonstrated that sexual fantasy and activity, because of naturally produced brain chemicals, has the ability to create brain tolerance to sex.

I have treated over a thousand male and female sex addicts. Almost all of them began with pornography. The number one source of pornography currently, and in epidemic proportions, is the Internet. It used to be that only men accessed sexually oriented web sites. Sadly, we are beginning to see an increase in the number of women who are addicted to pornography of all kinds, but mostly on the Internet.

The consequences of Internet pornography can be catastrophic. All of us who work in the field of sexual addiction have seen a marked increase in Internet addiction in the last year. Typically, our cases present as people who have lost jobs, vocations, and marriages due to Internet addiction. In a study of 91 women whose husbands were so addicted, for example, Jennifer Schneider, M.D. found that all felt hurt, betrayed, and rejected. All of these women felt unfavorably compared. 68% reported that their partner had become disinterested in sex with them. 22.3% attributed their divorce from these partners as due to the Internet.

As an addiction, Internet pornography can escalate. It may lead to other forms of sexual acting out. For some with accompanying personal pathologies, it may lead to sexual offenses. The physical and legal consequences to the addict and to others are obvious.

Finally, we should be aware of the dangers of Internet chat rooms as a place where sexuality can be problematic. We are aware that sexual predators can be present in chat rooms disguised in a variety of ways. Pedophiles may even send pornographic pictures to prospective child victims as a way of "softening" them up to eventual encounters. This has been a known form of pedophilic ritual for years. We have all warned our children against talking to strangers, but the Internet makes healthy decisions in this regard less likely. A number of well-known cases in which children and teenagers have been recruited for eventual sexual activity should warn us of the dangers of chat rooms.

Adults, also, may get caught up in chat rooms. I have a client whose husband gave her a computer for Christmas. She says that she doesn't remember the month of January. She became addicted to the "romance" of online chat. Researchers and experts in the field of romance addiction, such as Pat Carnes, Ph.D. have clearly describe that romance creates neurochemicals such as phenylethylamine (PEA) which would explain the addictive reaction of my client. My client's romance addiction escalated and she wound up actually meeting four of the men in person and developing a sexually transmitted disease as a result. I have had a number of clients who would fit this same profile.

On-line pornography and chat rooms appeal to those who are isolated, lonely and bored. When other emotional and neuro-chemical vulnerabilities are present addictions can be the result.

The Uniqueness of the Internet

One of the reasons that the Internet is so dangerous is because of its certain uniqueness. Al Cooper, Ph.D. (mentioned above) was the first to suggest the concept of the "Triple A Engine" of the Internet. He says that its uniqueness is that it is Accessible, Affordable, and Anonymous.

When I saw my first pornographic magazine, I had to be a detective to find what drug stores kept it in some hidden cabinet. As an adult I had to go to many fairly sordid places to find what I was looking for. The point is both as an adolescent and as an adult I had to go looking. Today, the Internet has made it completely *accessible* to the youngest of users. There are forms of pornography available today that weren't available even in the most perverse of locations just five years ago. Every year we see a rise in the kinds of material that are easily available. Many communities, such as my own in Minneapolis, are facing the problem of the easy accessi-

bility of pornography using computers in public schools and libraries. We are a free speech society. Recently, even the voters of a conservative city like Holland, Michigan rejected putting filtering devices on public library computers.

Internet pornography is *affordable.* We know that many people who may have paid for something originally can transmit it to others for free. We also know that many sexually oriented web sites offer free pictures as an enticement to log in with a credit card. Such free enticements led one of my clients to become addicted to sex on the Internet. He eventually spent $85,000 in the month of February. If there are people who might otherwise restrict their use of pornography, or various more expensive forms of it, because of money, there is enough free material available to keep them going. The majority of my clients who are addicted to Internet pornography don't pay for it.

Several psychologists, such as Dr. Mark Schwartz director of the Masters and Johnson Institute, have said that the *anonymous* nature of the Internet makes many more people vulnerable to it. He says that some who might not become compulsively involved in deviant sexual activities because of having to go to "dangerous" places and risking exposure, are now getting involved in the obscurity and "safety" of their homes. What this means is that more and more people are becoming more and more involved in sexually deviant forms acting out. It used to be than "normal" people might have an aversion to going to places that catered to sexual deviance, such as S&M bars. Now through on-line pornography, chat, and exchange, it is much easier to become involved in these activities.

To the triple A engine I would add a forth "A," *accidental.* Those who have sought to protect the free speech rights of pornographers have long claimed that it is an individual's free choice to view pornography. On the Internet, however, pornography may come looking for you. All of us are familiar with the unsolicited e-mails that advertise sexually oriented web sites. That is one thing. The greater danger for those who otherwise seek to use the World Wide Web for constructive purpose is that they will accidentally be exposed to sexually oriented cites.

Recently, for example, parents that I know told me the story of how their 8-year-old daughter was researching the fairy tale Cinderella on the web. She entered Cinderella in the search engine of her on-line service provider. She was given a number of options. One of them included the title, "See Cinderella for Yourself." This little girl of course wanted to see Cinderella, so she clicked in. She was immediately confronted with the picture of a nude female using a artificial penis to stimulate herself. I would consider this to be a form of sexual assault.

Robert Freeman-Longo, a well-known sexologist and researcher, conducted a recent study using AOL, the largest on-line service provider. He entered the words "parental control" into the search engine. 12.508 sites came up including a wide variety of sexually oriented ones. Can there be any doubt that even if you are looking for certain types of materials, they may accidentally come to you? Some might even question whether or not some of this is accidental. Estimates are that 85% of the production of pornography in this country is controlled by organized crime. Do we doubt that this faction of our culture would be aggressive in "purveying" their product?

As a recovering sex addict, I am personally offended by the aggressive and unique nature of Internet pornography. If I were an alcoholic, there would be no one bringing free alcoholic beverages to my door. Yet, in my work I have a professional need to be on-line frequently. I am assaulted daily by sexual opportunities that I have not invited into my life or pursued.

What Needs To Be Done

Briefly, let me suggest some points to think about concerning what might be done.

1. Regulation—As Americans we are generally afraid of censorship, as we should be. In that fear, however, we should not avoid the questions of when it might be necessary. To be truly free we should continually seek to control any form or oppression. It is clear to me, and many of my colleagues, that if we don't seek to regulate the cyber-sex industry, we are allowing a form of sexual abuse to continue unchallenged.

The law enforcement community in this country is capable of regulating pornography that is destructive. I would refer this committee to the report of Louis J. Freeh, Director of the FBI, to the Senate Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies of March 10, 1998. This report centered on effort to control the proliferation of child pornography. When we are in agreement that something is offensive and destructive we can devote energies that can bring it under relative control. Existing laws could be enforced if we could come to such agreement. Does there need to be special com-

missions to make recommendations as to what really are the dangers of Internet pornography?

2. Parent Education and Awareness—We might all agree that parents and child caregivers should be our main defense against children becoming involved in the dangers of the Internet. I would suggest however, that most parents are either ignorant of or apathetic toward the dangers of the Internet. Education and awareness similar to that provided about drugs, alcohol, and smoking seems appropriate.

3. Child Education and Awareness—Similarly, we should implement programs to educate our youth about Internet dangers similar to those that are available for drugs, alcohol and smoking. This might include the use of requiring that all sexually oriented web sites print warning on them similar to those that we require for tobacco. Remember, that this material may be addictive and, as such, even physical consequences are likely.

4. Mandate That Filtering Devices Be Used by Computers in Public Places—Given the four "A's" described above, we should especially protect children using computers in public places from getting assaulted by pornography. The same can be said for adults. Many kids may be able to "hack" around these filters, but that should not stop us from protecting those who can't.

5. Reward Employers Who Provide Filters At the Workplace—We are becoming more aware of the lost productivity that Internet pornography leads to. This is already having an impact on countless American businesses. We should encourage employers to educate employees about dangers, provide monitoring and filtering, and provide treatment for employees in trouble.

6. Fund Research About Effective Treatment of Internet Addiction—We already know that many of the forms of treatment that are effective with alcoholics and drug addicts can be applied to those who suffer with Internet pornography addiction. Little research exists to date about the specific modalities that are beneficial with this population. Since this is a growing problem, we need to act now. My belief is that we need to be concerned about the supply of pornography on the Internet, but that we must be equally concerned about the supply.

7. Tax Pornographic Web Sites—Monies from the taxation of alcohol and tobacco are used for research, treatment, and education. Why could this not also be done for pornography? All of my other recommendations could be funded by such a tax. We should be willing to enter the debate that will inevitably ensue as to what is pornographic. There are enough sites that are obviously pornographic to the vast majority of Americans to begin with

I believe that Internet pornography is a great plague on this nation. I hope that these observations are helpful to the committee. I am willing to answer any questions and to provide members with any specific references to research that I have quoted.

Mr. TAUZIN. We will take one more witness before we do a half-hour break for these three votes that will be on the floor. So we will go now to Mr. Robert Flores, vice president and senior counsel of the National Law Center. Mr. Robert Flores.

STATEMENT OF J. ROBERT FLORES

Mr. FLORES. Mr. Chairman, honorable members of the committee, thank you for providing me with an opportunity to testify this morning on the important and troubling issue of the explosive and uncontrolled growth of obscenity on the Internet. In my career as an assistant D.A. In Manhattan, acting deputy chief of the Department's Child Exploitation and Obscenity Section and as a special law enforcement advisor with the National Law Center, and now as a commissioner on the congressional COPA commission, I have seen the vicious tactics of the pornography industry, the syndicates, and the destruction that they hand out, as well as the actions of pedophiles, and I am sure of one thing: that law enforcement has value, and effective law enforcement will be able to deal with a substantial amount of this criminal problem.

I know that vigorous and fair enforcement of the law can solve many of those problems when prosecutors use the laws given to them by the Congress.

In the past 5 years, much has changed about the industry. In late 1995, few of the major pornographers had a major presence on the Internet. While the amount of material that was then available was overwhelming, today it is available in quantities and formats which make it a ubiquitous commodity. Today, obscenity merchants have become so bold because of the lack of action by the Justice Department that they have gone public, and I mean public, by being on the NASDAQ, launching IPOs on the New York Stock Exchange, and Forbes magazine, as well as Forester Research and other publications report that pornography to the tune of $1 billion already flows over the Internet and it is expected to double or triple within the next 1 or 2 years alone.

In addition to the change in the amount today, adult pornography sites have moved to feature as a predominant theme sexually explicit material which is marketed as depicting teen, young, Lolita, virgin and high school girls and boys. The term "barely legal" is all over the Internet. Now, many of these terms were once the sole province of child pornographers. Yet this jargon and code has become a stable of adult obscenity marketers.

Pornographers are also the most aggressive marketers. They have used newly developed push technologies, alongside offensive and fraudulent marketing ploys. The Internet user community is bombarded with advertisements, tricked into visiting sites, given hot links to porn when search engines are asked for innocent sites, sent unsolicited porn spam e-mails and trapped in endless mousetraps that bounce them from porn site to porn site when they try to leave.

In spite of all of this, the Department of Justice has refused to take action, in spite of the fact that the Congress has specifically earmarked a million dollars for activity to target obscenity online. It is critical that the Congress understand and recognize that the refusal of the Justice Department to enforce existing obscenity laws is unjustified and inexcusable.

In 3 short years, between 1989 and 1992 approximately, we were able to prosecute more than 120 major obscenity distributors and we took in more than $21 million in fines and forfeitures. The obscenity test works. These prosecutions are difficult. They do need expertise but it can be done. And the record should be clear that there is no question that the test that is going to be applied is the same test that was applied in 1989, in 1992, and has been applied by State and local prosecutors throughout the United States over the past years.

As the Supreme Court stated in Reno, transmitting obscenity, whether via the Internet or other means, is already illegal under Federal law for both adults and juveniles. The reach of this criminal prohibition is also the same. Thus we can prosecute obscenity where somebody stores it on their computer, any District through which it travels on the Internet and the District into which it is received.

In 1996, Chairman Hyde moved to make sure that it was clear to everyone, including Federal prosecutors, that Federal laws apply and Congress amended sections 1462 and 1465 of Title 18 to specifically include interactive computer services. Now, we weren't powerless before that. The Thomas case, which the Justice Depart-

ment will probably talk about, was prosecuted before that amendment under existing law because it is illegal to use wire communications, the telephone lines.

Finally, even the question of foreign transmissions into the United States has been answered. Most of the world's hard-core obscenity comes from America's porn syndicates, and they are subject to U.S. Law no matter where they send their criminal materials to or from. Hiding their Web servers overseas won't save them. We can prosecute American criminals in U.S. district courts and seize their assets.

Contrary to complaints made by some, our law reaches overseas. As a practical matter, we can prosecute Web site owners who directly profit from the exploitation, the people who produce and distribute the movies, even the recruiters and procurers of women who run virtual prostitution operations, making live images available, and finally those who bankroll this industry.

Our Constitution protects speech, not obscenity, and the President and the Justice Department in particular must recognize that difference and fulfill their obligations. I would ask that the appendices also to my written record be included in the record.

Mr. TAUZIN. Without objection so ordered. The Chair thanks the gentleman.

[The prepared statement of J. Robert Flores follows:]

PREPARED STATEMENT OF J. ROBERT FLORES, VICE PRESIDENT AND SENIOR COUNSEL, NATIONAL LAW CENTER FOR CHILDREN AND FAMILIES

Mr. Chairman and Honorable Members of this Committee, thank you for providing me with an opportunity to testify this morning on the important and troubling issue of the explosive and uncontrolled growth of obscenity on the Internet. In my career as an Assistant D.A. in Manhattan, acting Deputy Chief of the Department of Justice's Child Exploitation and Obscenity Section, as a special law enforcement advisor with the National Law Center for Children and Families, and now as a Commissioner on the Congressional COPA Commission, I have seen the vicious tactics of the pornography syndicates, the destruction handed out by pedophiles, and the value in effective law enforcement over the years. I believe in the law as an answer to criminal social problems and I know that vigorous and fair enforcement of the law can solve many of those problems when prosecutors use the laws given them by their Legislatures.

It is obvious that the uncontrolled growth of this criminal activity must be effectively addressed, and soon, or Congress will continue to be confronted with the need for increased regulation, rising levels of sexual abuse and dysfunction in adults and children, increased health care costs to treat those dysfunctions and the victims of sexual abuse and addiction, the poverty that results from broken homes and marriages over sexual abuse and addiction, and even the slower growth of Internet use by children and families who are rightly afraid of its dark side.

In the past five years, much has changed in the size and nature of the Internet based pornography industry, mostly on the World Wide Web and Usenet newsgroups. In late 1995, few of the major pornographers had a major presence on the Net. While the amount of material that was then available was astounding by anyone's count, today it is available in quantities and formats that make it a ubiquitous commodity. Today, obscenity merchants have gone public, as in the NASDAQ and other capital markets. Forbes reports that "pornography to the tune of $1 billion already flows over the Internet."

In addition to the change in the amount of material on the Internet, a look at what now comprises a sizeable and growing portion of hard-core obscenity, should send shivers up the spine of every person of good will. Today, adult pornography sites have moved to feature, as a predominant theme, sexually explicit material which is marketed as depicting "teen", "young", "Lolita", "virgin", and "high school" girls and boys. Once the sole province of child pornographers, this jargon and code has now become a staple of adult obscenity marketers.

Does this threaten children? You better believe it does. Our kids and grand-kids see it and become indoctrinated by it. Pedophiles and porn addicts see it and become incited by it. Even the U.S. Supreme Court recognized that the mere existence of child pornography images is an ongoing danger to children, because of the stimulating effect it has on pedophiles and the seductive effect it has on children. *See Osborne v. Ohio,* 495 U.S. 103, at 111 and n. 7 (1990). That's why Congress criminalized the possession of child pornography in Title 18, U.S. Code, Section 2252, and added computerized child porn in Section 2252A. How strange indeed, if alone among all other speech, adult obscenity did not also stimulate and encourage people to action.

The pornography industry has also become among the most aggressive marketers on the Internet, using newly developed "push" technologies alongside offensive and fraudulent marketing ploys. Thus, even if it were ever true, and I doubt it, that only those who sought out obscenity could find it, today only a lucky few are able to avoid it, as the Internet user community is bombarded with advertisements, tricked into visiting sites, given hot links to porn when search engines are asked for innocent sites, sent unsolicited porn spam e-mails, and trapped in endless mousetraps that bounce them from porn site to porn site when they try and leave.

In spite of the explosive growth in the distribution of obscenity, aggressive marketing efforts which assault and trap unwilling Web surfers, and a focus on material which portrays children as a suitable sexual interest for adults, the Department of Justice has refused to take action.

It is critical for the Congress to recognize that this refusal of the Justice Department to enforce existing obscenity laws is unjustified and inexcusable. Members of this Congress and your predecessors have provided the tools and means to address this problem, but those federal statutes are not being used.

The record should be clear that there is no question as to what the test is that will be applied when prosecutions are brought involving Internet distribution or pandering of obscene material. Even in the Communications Decency Act and Child Online Protection Act cases, cases which are well known to the pornography industry, the Supreme Court and federal District Courts, recognized that federal obscenity law, based on the *Miller* test, applies to the Internet. As the Supreme Court stated in *Reno v. ACLU,* 521 U.S. 844, 117 S.Ct. 2329, 2347 n. 44 (1997): "Transmitting obscenity and child pornography, whether via the Internet or other means, is already illegal under federal law for both adults and juveniles." While this is not a point to which some may want to draw attention, that is the law. Moreover, those courts offered enforcement of existing obscenity and child pornography laws as part of the solution to the problem of protecting minors from sexually explicit material. Moreover, the Department of Justice represented to the courts that they would do so, though they have yet to prosecute a single case of substance.

Just as the test for obscenity remains the same, the reach and applicability of the criminal prohibitions to Internet distribution and pandering of obscenity also remains the same. Thus, someone who sells obscenity may be prosecuted in the place where he stores the material on his computer, any district through which it passes, and the district into which it is received. Under Section 1462, for instance, it is a felony to use the phone lines and other communications carriers and facilities of interstate and foreign commerce to knowingly upload, download, or transmit obscenity.

In 1996, in order to clarify that federal laws apply to the Internet, Congress amended Sections 1462 and 1465 of Title 18 and specifically included "interactive computer services" among those facilities which may not be used to traffic obscenity. Even then, the Department was unwilling to move forward to address this criminal activity and in four years not a single Internet based obscenity case has been brought by main Justice.

Finally, even the question of foreign transmissions into the United States has been answered and there is no serious debate that we cannot reach conduct which originates in foreign countries. The frequently heard argument that we really can't do anything about Internet obscenity because so much of it comes from overseas is specious. Most of the world's hard-core obscenity comes from America's porn syndicates and they are subject to U.S. law no matter where they send their criminal materials from or to. Hiding their Web servers overseas won't save them, we can still prosecute American criminals in U.S. District Courts and seize their assets and credit card receipts from U.S. banks. Moreover, I can't imagine it could be used by the Justice Department to justify its lack of effort. For in testimony on March 9, 2000, before the Committee on the Judiciary, Deputy Assistant Attorney General Kevin Di Gregory, took justifiable pleasure in announcing that the week before his testimony, "a jury in federal district court in New York found Jay Cohen, owner of an Internet gambling site in Antigua, guilty of violating 18 U.S.C., section 1084, a

statute that makes it illegal for a betting or wagering business to use a wire communication facility to transmit bets or wagers in interstate or foreign commerce."

Contrary to the complaints made by some, the courts have consistently made clear that federal obscenity law applies in cyberspace as it does in real life. Thus, the answer to the question of who and what may be prosecuted under federal obscenity law is as well known to the ACLU and pornography industry lawyers as it is to Government prosecutors. Title 18 sections 1462, 1465, 1466, 1467, and 1470 apply to Internet distribution and pandering and may be used today by prosecutors interested in protecting children and families from this scourge.

As a practical matter, I believe that federal investigators and prosecutors can and must bring cases which would make a difference for average families and which would be a giant step towards stopping sexual exploitation. For example, prosecutions can be brought against the Web site owners who most directly profit from this form of human exploitation. The producers and distributors of movies, pictures, and other obscene material who wholesale them to the Web sites for resale can also be pursued under existing law. The recruiters and procurers of women who run virtual prostitution operations making live images available through the Internet may also be prosecuted for transmitting obscenity. And finally, those who bankroll these operations, many of whom have historically been organized criminal operations, may also be investigated and prosecuted.

Leaders and businesses in Europe, Asia, Latin America, and our other trading partners look to the United States to see what we, the major source of obscenity worldwide, will do with this form of exploitation. In fact, there is a 1911 Treaty on the Suppression of Obscene Publications that would provide an existing framework for international cooperation to deal with hard-core obscenity on the Internet and World Wide Web.[1] That Treaty is still in force and now has at least 126 member countries as signatory nations, including most of the Americas, Europe, and Asia. We seek to lead in every other Internet related area, why not here as well. Can money be made by this industry? Of course. In fact, it is one of the few guaranteed ways to succeed financially on the Internet. But at what cost? It is not free, either to the people who consume the products or the society where it runs rampant. We cannot fail to lead simply on the assumption that some amount of obscenity comes from overseas. To do that would be to turn over our Country and its safety to pornographers and sex business operators who are savvy enough to move their servers and remote offices overseas. We don't do it in any other area of criminal law, why would we start here?

Our Constitution protects speech, it does not protect obscenity. The President and the Justice Department in particular must recognize that difference and fulfill their obligation to pursue violations of the laws passed by Congress. Mindlessly investigating and prosecuting cases, whether child pornography, child stalking, or even obscenity, will not make children and adults safe from being assaulted by material that is not only offensive but illegal. A comprehensive and coherent strategy which addresses each of the major aspects of the obscenity and sex business operations is necessary. Whoever is blessed with the opportunity to lead in November will bear the responsibility of choosing a path down which we will all walk. It is hard to imagine leadership on this issue being worse than today, when the pornography trade association is able to ask the question in its March 2000 trade publication, "how likely is it, would you say, that we are going to enjoy the same benevolent neglect that the industry has enjoyed under Janet Reno?" It is shameful that the American porn industry has come to look at law enforcement in that way.

Thank you for the opportunity to address this Committee, and I would be pleased to answer any questions you may have.

Mr. TAUZIN. Let me ask you all now to stand down for a half hour. We understand there are 3, possibly 4 votes on the floor. We will reconvene in a half hour. So we will come back at 11:10, and we will reconvene with this panel, complete it, and then invite our second panel.

We thank you very much. The committee stands in recess.

[Brief recess.]

Mr. TAUZIN. The subcommittee will please come back to order. We will ask our witnesses again to take seats. As we recessed, we had just heard from Mr. Robert Flores, vice president of the Na-

[1] Agreement for the Suppression of the Circulation of Obscene Publications, 37 Stat 1511; Treaties in Force 209 (US Dept State, Oct 31, 1956).

tional Law Center, and we are now going to hear from Tracy Stewart, the head of technology, FamilyClick.com. Again, our admonition is to please adhere to the 5-minute rule. Ms. Stewart, you are recognized.

STATEMENT OF TRACEY R. STEWART

Ms. STEWART. Good morning, Mr. Chairman and members of the subcommittee. My name is Tracy Stewart, head of technology for FamilyClick, a nationwide filtered Internet service provider and family oriented Web site. The role of our company is to provide for families that have freely chosen filtered access to a safe Internet experience.

Filtering used to be easy, but due to the bold and aggressive marketing by the porn industry of their product, very sophisticated software and hardware is now required to do our job. I will quickly discuss several techniques used by the porn industry which causes technological challenges for filter companies and makes it virtually impossible to guarantee a safe online experience. I will provide complete details of the techniques in my written testimony.

Spam. Mail addresses are harvested by bulk e-mail and from many places on the Internet: chat rooms, message boards, auctionsites such as eBay. Book mailing lists are inexpensive for the pornographers to purchase. The goal of the pornographer is to send out millions of unsolicited messages containing, for example, a sample image and link to a porn site. They know most will not generate a positive response, but due to the sheer volume of mail sent, they will pick up some customers. A 10-year-old boy is just as likely to get the unsolicited porn message as a 40-year-old man. Over 30 percent of unsolicited e-mail contains pornographic information.

Banner ads. Many legitimate Web sites that would not be blocked by filters carry banner ads to porn sites. Also, once on a porn site, it may contain dozens of ads to other porn sites. Porn sites have developed an almost unbroken circle of links between each others' sites which maximizes their profitability and traffic. Once on a porn site you have access to dozens, if not hundreds, of other porn sites.

Innocent or innocuous or misspelled domain names. These porn Web masters have registered many innocent sounding names that you would not expect you would need to filter: Boys.com, girls.com, coffee bean supply.com, BookstoreUSA.com, and the infamous WhiteHouse.com. These all lead to very explicit and graphic porn sites. Also legitimate companies which spend millions of dollars building brand names, porn Web masters commonly register misspelling of these brand names. For example, my favorite is Yaawhoo.com, takes you to a porn site.

Suggestive or graphic exit consoles. Once you stumble into a porn site, leaving may not be easy. Normally you would just hit the back button on your browser, but many porn sites force you to continue to look at what they have to offer by opening new windows each time you close a window, and each one has an image or invitation to preview or join. Each window you close opens up another new window. They are hoping you will find something you like while you are trying to exit. Sometimes these windows completely lock up

your PC and system resources, forcing you to reboot and maybe lose any unsaved information you had.

The final one is search engine manipulation. Meta tags are short descriptive comments placed in a Web page. They are not displayed when you view a page. They are placed there by the programmers and developers of the Web page. Many search engines use these meta tags to categorize a Web site. There are no rules that say a meta tag description has to match the content on the site. Porn sites often use common search terms such as brand names in their meta tags to get higher placement or recognition within the search engines. A porn site can have a meta tag of family friendly, safe ISP if they want.

How can our users protect themselves? First of all, you cannot use the Internet, which is really not an option in today's society, or you can use a service that offers a whitelist, which is a very restrictive list of preapproved sites really only appropriate for small children. Filters installed on home computers put the responsibilities completely on the parent to maintain the software and the subscription to a filtering list.

Then there is service site filtering where all the filtering lists and software resides outside the home. The burden is removed from the parent but it is up to the technology industry to keep up with what the pornographers are doing. Families bring filters into their home to protect, not to censor, their family. They also expect them to work 100 percent of the time. Believe me, I have found that out.

The aggressiveness of the pornographers present a technological challenge that we, the filtering companies, are constantly trying to keep up with. Our goal is to provide the safest possible experience for our customers while online.

This concludes my statement.

[The prepared statement of Tracy R. Stewart follows:]

PREPARED STATEMENT OF TRACY R. STEWART, HEAD OF TECHNOLOGY, FAMILYCLICK.COM LLC

Mr. Chairman, members of the committee, I am Tracy Stewart, Head of Technology at FamilyClick.com LLC; a nationwide filtered Internet service provider based in Virginia Beach, VA. I would like to thank you for the opportunity to speak with you today concerning a subject that I, my co-workers, and family and friends have spent a great amount of time dealing with. That is the growing influence that the online pornography industry has on this wonderful new learning tool that we know as the Internet.

Background

Almost everybody realizes that pornographic web sites are out there. The sex trade is arguably the world's oldest profession and has long been one of the most profitable. Its influence has been felt within every culture since the beginning of recorded history and it should come as no surprise that the porn industry has established a strong foothold in cyberspace. Pornography was the first consistently successful e-commerce product and the online porn industry is credited with pioneering many of the security, electronic payment, advertising and site management techniques that are used today by mainstream web site operators.

Many believe that the online porn industry operates in a niche; hidden away in a back room and visible only to those who come looking for it. In reality, nothing could be further from the truth. Free of the restrictions that pornographers in the print, film and paraphernalia industries face, the online pornographer has become very bold and aggressive when it comes to marketing his product. He is willing to force his message to be viewed by thousands, even millions, of unsuspecting persons, both young and old, because he knows that some of these people, perhaps only a

few, will eventually become his customers. He is willing to trick you into visiting his site when you are really looking for something completely different because he knows there is a slight chance that you will like what he has to offer. And he is willing to hold you hostage when you stumble through his door because he knows that you might just give in after your first attempts at escape fail.

As a businessman, the online pornographer has the same goals that any legitimate businessman has: profits. But without the legal, social and moral restrictions to hold him back, the online pornographer has aggressively and ruthlessly marketed his product and now ranks third in total sales on the Internet; trailing only computer products and travel.

Formula For Web Site Success: Traffic = $$

One of the first goals of any web site operator, whether the site is "legitimate" or pornographic, is to generate traffic or "hits" to that site. Without hits, the commercial electronic storefront will not have any customers and the free portal will not have many ad impressions. With over four thousand new web sites coming online every day, generating traffic is a much more difficult task than it appears on the surface. Competition for traffic is fierce and even with the advent of faster networks, more efficient software and swifter computers, users only have so many hours in a day in which to explore the web. The site that adheres to the "If I build it, they will come" principle is doomed to fail.

Pornographic web site operators have been pioneers in the field of web site traffic generation and have come up with some very imaginative, and often aggressive, methods of driving traffic to their sites. In fact, many of the techniques currently used by legitimate sites to increase traffic were first implemented and perfected by pornographic web sites.

What the Porn Industry is Up To

Pornographic web site operators have been so successful in generating traffic for their web sites that it is now virtually impossible to spend any significant amount of time surfing the web without stumbling across pornographic or otherwise offensive web sites. In fact, it has now become a challenge to get through an online session without encountering lewd, vulgar or risqué sites. Increasingly, the expectation of many adults and most teen aged web surfers is that they will encounter at least one inappropriate web site during a typical online session. And for those that are looking for online porn, it's only a mouse click away.

Lacking the fear of prosecution, pornographic web site operators have perfected methods of generating traffic to their sites that are often as offensive and immoral as the material they are attempting to promote. Employing methods meant to deceive, lure, tease, trick and capture, new porn web sites can expect a steady flow of traffic in a fraction of the time that it takes a legitimate web site to generate the same amount of traffic.

Spam—One of the earliest and most time-honored methods of increasing exposure and generating traffic for a porn site is spam; the sending of thousands, or even millions, of unsolicited email messages or Usenet postings. It is estimated that over 30% of all unsolicited email messages are pornographic in nature. In many Usenet newsgroups, close to 100% of the postings are advertisements for a pornographic web site. These messages and postings often include an attached binary image intended to serve as a "free" sample of what's available on the main web site.

Spamming is, perhaps, one of the easiest known methods of web site promotion. The creation of mailing lists for the purpose of unsolicited bulk mailings has grown into a healthy cottage industry. Bulk emailers harvest email addresses from Usenet postings, message boards, auction sites such as www.ebay.com and www.bid.com and from less than reputable bulk email "opt out" or "unsubscribe" services. These mailing lists cost pennies to generate and are easily affordable by web site operators with the most modest of budgets. Bulk mailing and posting software is also very affordable and easy to setup and operate. To add insult to injury, the messages are usually delivered to the victims by "borrowing" the services of an unsuspecting third party that installed an email server and forgot to turn off third-party mail relay. The spammer then delivers his message to thousands, or even millions, of people who did not ask to receive it and uses the networking and computing resources of an innocent bystander to do all the grunt work.

Bulk emailers do not lose a lot of sleep worrying about targeting their mailings. Since they are paying next to nothing to send their messages out, they are more concerned with volume than they are with hitting a particular target audience. A ten year old boy is just as likely to receive an email message explaining the virtues of the latest weight loss plan as he is a message exhorting him to visit Bambi's Naughty Playground. He may not actually visit the site but the free sample picture

of Bambi cavorting with her friends won't be easily erased from his impressionable mind. Bulk mailers expect that the vast majority of their messages will not generate a positive response. All they are looking for is a handful of adults with credit cards handy so they can recoup their small investment.

Banner Ads—By now, everyone who has spent any time on the web has seen banner ads. Many of the worlds most visited web sites derive all or a major portion of their income by displaying these ads. These click-through images that bring the surfer to other sites translate to real traffic and money. But it was the online porn industry that originated and perfected the use of the banner ad. Today, the online porn industry continues to pioneer new and often revolutionary methods of using online banner ads.

Go to almost any adult web site and you will see, prominently displayed, dozens of ads linking to other pornographic web sites. By any definition, these are ads for competitive sites. While General Motors might not be willing to place a link to a Chrysler web site on its page, such an arrangement is not only common in the online porn industry, it is expected. All a surfer needs to do is wind up on a single adult web site, which is very easy to do, and he's got easy access to dozens, if not hundreds, of additional sites. While you would not expect Macy's to send you to Nordstroms" web site if they don't have the pair of shoes you want, you can expect a porn site specializing in blonde's to direct you to a site featuring redheads if that's what you prefer. The almost unbroken circle of links developed by the online porn industry has proven very effective at maximizing profitability and traffic.

Porn sites have gone beyond the easily abused pay-per-click payment system, which is commonly used by legitimate web site operators. Arrangements to pay the referring partner a flat fee or a percentage of the first sale are becoming prevalent. Often there is no money involved and deals are consummated over a drink and a handshake. This cooperation is more than a traffic and revenue generating technique in the online porn industry; it is interwoven into the very fabric of the industry.

Banner ads for pornographic web sites don't appear only on other porn sites. Legitimate sites, hungry for the dollars paid out by porn operators, often eagerly place these ads on their own sites. Porn ads placed on legitimate sites are normally less graphic and suggestive than the ads that porn operators share with each other. But the sites that these "clean" ads lead to are every bit as offensive as the sites advertised by the more graphic ads.

Innocent or innocuous domain names—It often is not very difficult to determine the address for a particular web site. For example, FamilyClick's web site is at www.familyclick.com and the web site of the National Football League is at www.nfl.com. Many users can derive these site names without the need to resort to search engines or web directories. Most experienced users try obvious domain names directly. But that doesn't always yield the expected results.

Consider "Teenagers Hideout". Seen in a TV listing, one could safely assume that Teenagers Hideout was a new addition to the Nickelodeon Television lineup. At Barnes and Noble, it could easily be the title of the latest installment in the Goosebumps series. A parent who's teenage daughter wanted to watch "Teenagers Hideout" on Nickelodeon or buy the "Teenagers Hideout" paperback at the local mall probably wouldn't feel alarmed. But there is no such presumption of safety in cyberspace. The web site www.teenagershideout.com redirects the surfer to the PrivateTeens.com porn site.

Unencumbered by ratings systems or V-Chips, porn webmasters have registered many innocuous or innocent sounding domain names for their sites. Boys.com, teens.com, coffeebeansupply.com and bookstoreusa.com all lead to very explicit and graphic porn sites. While legitimate web site operators strive to come up with domain names that are meaningful and descriptive, porn webmasters just try to cover as many bases as they possibly can. The legitimate webmaster wants you to visit his site when you are looking for the types of goods or services that he offers. The porn webmaster wants your traffic regardless of your reason for being on the net.

Misspelled Domain Names—With domain names being sold for hundreds of thousands, and even millions, of dollars, it is perhaps not surprising that the porn industry should try to take advantage of the goodwill and trust that legitimate companies have spent years building. For example, the creators of Yahoo! probably never imagined that a site dedicated to nude photos of Britney Spears would be parked at www.yaahwho.com. The Internet is full of sites that can be accessed by using a common misspelling of a popular web site. Not surprisingly, most of these misspelled web sites are pornographic in nature.

Porn site operators have become experts at taking advantage of some of the more common and predictable mistakes that people make. If a student just introduced to keyboarding places his or her hands on the wrong keys, chances are a pornographer

has it covered. How about the middle school student doing research on the President of the United States and goes to www.whitehouse.com instead of www.white house.gov? The porn industry has taken care of that common error. And if you're looking online for information about Disney, check your spelling carefully because www.dinsey.com and www.dinseyland.com won't get you to the Magic Kingdom.

Suggestive or graphic exit consoles—Once an innocent surfer stumbles across a porn site, all the work getting him there will be lost unless they take some steps to keep him from leaving. Porn webmasters have become experts at building one way doors leading to the Internet's Red Light district. Did you end up at a site that you didn't intend to visit? It is normally not a problem; just hit the back button or close your browser window and you're right back where you started from. But if the site that you accidentally ended up at happens to be a porn site, you may not be able to check out as easily as you checked in. Hitting the back button or closing the browser window commonly results in the opening of one or more 'exit consoles'; each a new browser window showing you a site of the webmasters choosing. Many of these exit consoles are at least suggestive; if not graphic. Many feature "free preview" buttons that lead to the creation of still more browser windows.

An example is the web site www.highsociety.com which bills itself as "The All Sex and Celebrity Web Site". The initial page displays a warning about "explicit adult content to date banned from the U.S." and it admonishes the viewer that he or she MUST be 18 to enter. But, 18 or not, at this point you've already had an eyeful, you're already in and you can't easily leave. Clicking the back button causes another browser window to pop up; this one features the "Lust Highway" site. Close the Lust Highway window and it is quickly replaced by the Chateau deSade site which features "Hardcore Sado-Masochism". That is followed by visits to sites offering "Free Porn and Screensavers", "The Youngest Girls Allowed by Law" and a site "Where All Your Sexual Fantasies Come Alive". All together, the surfer leaves the High Society site by way of 13 sexually explicit and graphic porn sites. Each site features a graphic image on its front page and each gladly accepts credit cards.

The "Thirteen Steps Through Paradise" exit route employed by High Society is actually one of the easier and less obtrusive exit plans used by the porn industry. The thirteen windows used to leave High Society open up one after the other with the closing of each window leading to the birth of exactly one successor. Other sites employ as many as 23 new browser windows. Often a porn sites exit plan will involve the creation of a dozen or more exit consoles, all starting up at the same time and competing for the systems resources. New windows are created as fast as the user can close them. In many cases, this causes the system to lock up forcing a reboot; often resulting in the loss of unsaved work.

The damage often goes beyond the lost work and the possible harm caused by rebooting your system. As pages and images are downloaded from the net, they are cached onto your systems hard drive. This speeds up access during subsequent visits to a web site as the information stored on the hard drive can be displayed if the information on the site itself hasn't changed. Since the cache contains pages and images from sites that you've intentionally visited as well as those that you ended up at by accident, any person with access to the computer can view these images without even being online. Many users do not even realize that these images are there and would be appalled to learn that such material actually resides in their home.

The porn industry takes advantage of a technique known as Javascript Slamming to make this happen. Using onLoad and onUnload methods, they can open new windows upon entry to or exit from a site. The onUnload method is particularly iniquitous in that there is no escape. It's possible to turn off the execution of Java entirely from within the browser. Unfortunately, doing so blocks about 50% of the good content available on the net. Browsers, such as Opera, can be configured to never open new windows. Again, disabling this feature is equivalent to disabling much of what is available on the Internet. Not going to porn sites is one way of avoiding the exit console syndrome. But since many porn site visits are the result of an accidental wrong turn in cyberspace, avoidance isn't a very effective treatment for the problem. And many non-porn sites, particularly sites dealing with online gambling, have learned from the porn webmasters and adopted the Javascript Slamming technique for their own purposes.

Manipulating Search Engines—Most web site operators, legitimate and otherwise, spend a great deal of time trying to describe their site by means of meta tags. Meta tags are short descriptive comments placed within the body of a web page. Not readily visible using most browsers, meta tags contain the keywords and descriptions used by search engines to categorize web sites. Using FamilyClick as an example, the keywords chosen were those that accurately describe the content offered on our site and the filtered ISP service offered.

Unfortunately, there is no rule that requires that a keyword placed in a meta tag has to accurately describe the site. The porn site www.girls.com uses teens as a keyword as does FamilyClick. So a surfer looking for information related to teens would be just as likely to find www.girls.com as he would www.familyclick.com. While mainstream web sites strive to use descriptive keywords, porn web site operators use whatever the search engines are currently indexing. By posting hundreds of test pages, porn operators can readily determine what the major search engines are looking for. They then load up their sites with meta tags this month, titles the next, and meta descriptions the month after that. Many of these sites are temporary portal sites customized for a particular search engine. These portal sites contain nothing more than the information that the search engines want along with a redirect to the actual site. Since the porn webmasters are so good at generating traffic, when a portal site has outlived its usefulness, it is quickly replaced with another.

And when it comes to spamming, the porn industry does not stop with email and Usenet. They routinely spam the search engines by submitting every page and subpage that makes up their site, as well as hundreds of throwaway portal sites. Since the search engines will eventually detect this spamming, porn operators are careful not to use their actual site. They use phony portal sites that can be replaced without any trouble.

Usenet—Before there was a World Wide Web, there was Usenet, commonly referred to as newsgroups. Originally intended as a huge worldwide bulletin board where users could discuss a wide variety of topics, Usenet has grown into a system where users can share not just thoughts and ideas but files. Not surprisingly, an increasing percentage of these files are erotic images, videos and sound clips. Of the almost 36,000 groups carried by one major provider, almost 600 are described as having content related to sex and another 500 carry content which is erotic in nature. There are newsgroups specializing in various fetishes; groups specializing in bestiality; groups that focus on various parts of the body and, for material that just doesn't fit anywhere else, groups that desire tasteless pictures and stories. The trick of misspelling domain names probably originated with Usenet; the group alt.binaries.pictures.boys.barefoot carries images of young boys with nothing on their feet. Not surprisingly, it isn't only shoes that some of these boys are going without. Many of the 12,000 or so groups in the alt hierarchy are almost exclusively dominated by material that is sexual in nature.

As an open system, anybody can post almost anything to any Usenet group. While the posting of a message related to British soccer may not be welcome in a group devoted to the breeding of tropical fish, it's difficult to prevent off-topic posting. A user looking through a Usenet group intended for web browser discussions is just as likely to come across a nude image of a young actress, as he is information on the latest Microsoft Explorer bug. The pornographers are well aware of this fact and they habitually flood almost every newsgroup with free samples and other enticements to visit their web sites. This has gone far beyond spam, as many groups now carry nothing but invitations to come visit various web sites. Using high throughput systems, porn operators pump out gigabytes of graphic content.

Besides serving as a method of increasing hits to a site, Usenet is also a rich mother lode of content for the porn webmasters. Usenet is full of images, videos, stories, jokes and other material. Much of this is posted by amateur photographers and videographers and consists of pictures of wives and husbands, girlfriends and boyfriends, the girl or guy next door, couples, trios, dogs, cats, hamsters as well as all sorts of inanimate objects. With the introduction of affordable digital cameras, scanners and web cams, the amount of material waiting to be harvested by a porn webmaster is increasing everyday.

Avoiding the Net's Dark Side

The most sure-fire method of avoiding the seedy part of the net is to stay off the net altogether. If your computer isn't hooked up to the net, the only way that porn can work its way into your system is if someone carries it in on a diskette. But staying completely off the net denies access to a powerful learning and entertainment tool. There are methods of taking advantage of what the net has to offer while still offering your family some measure of protection from the aggressive online pornographers.

Whitelists—A whitelist is simply a list of pre-approved web sites that have been checked and determined to be safe. Some Internet Service Providers offer a service that restricts its users from going to any site not listed on its whitelist. Current database technology allows whitelists to be quite large and can be updated and searched in almost real time.

But with over four thousand new web sites coming online everyday, maintaining a whitelist and keeping it up to date is a major challenge. Since it's already known

that the name of a site is not necessarily indicative of its contents, each site needs to be manually visited in order to determine if it should be included on a whitelist or not. And since the contents of a site may change over time and domain names are often sold, each site on the list needs to be revisited periodically to ensure that it still merits inclusion in the list. However, as long as the whitelist is properly maintained, it is a very effective method of protection.

Due to these challenges, whitelists are only appropriate in limited numbers of cases. The most common application of a whitelist is to ensure safe Internet access for small children. FamilyClick offers, as one of its access levels, access to a pre-approved list of sites which have been determined to be appropriate for children seven and under. The FamilyClick Children's Playroom is 100% safe but would not be appropriate for an experienced user who may need to use the web for research.

Local Filtering—A local filter is a software program, installed on a users computer, that monitors a users Internet activity and decides whether to allow that activity or not. The filters normally compare web addresses, email addresses and Usenet group names against a list of blocked addresses. If the address does not appear on the list, access to that resource is permitted. Some local filters utilize word lists as well as address lists.

Local filters have many of the same problems that whitelists have and are usually much less effective at blocking inappropriate material. Lists need to be maintained and the sheer volume of new web sites being launched means that new porn sites might not be listed for weeks or months. Often users are required to maintain a subscription in order to ensure that the list is kept up to date.

The main problem with local filters is that they are installed on a users computer. Many parents purchase copies of filtering software only to hand it to a tech savvy teenager to be installed. Although some local filters are password protected, they can be defeated either by removing them entirely or by renaming a few files.

Proxy Filtering—The most effective filter is a filter that resides on a server outside of the home. Often known as a server based filter, the proxy filter operates by intercepting all requests from a user and then deciding whether to pass the request on or not. Proxy filters utilize lists of blocked sites as well as word lists. Server based filters can take advantage of the latest database technology to maintain lists of blocked sites and banned words. The most advanced proxy filters scan outgoing web requests and incoming web pages and perform context searches rather than simple word searches. This provides protection against sites too new to have been catalogued.

Proxy filters are commonly used in businesses and educational institutions where the network administrator can force the traffic to flow through the filter as it travels to and from the users. In this type of setup, a proxy filter is very difficult, if not impossible, to defeat. Users can either access the net through the proxy filter or not at all.

Increasingly, filtered Internet Service Providers are utilizing proxy filters to protect their subscribers from unwanted pornography. Several, such as FamilyClick, utilize various levels or tiers of filtering. This allows parents to decide the level of access that is appropriate for each of their children. FamilyClick and other top providers force all the network traffic from subscribers to flow directly through their proxy filters. A tech savvy teen that attempts to bypass the proxy filters finds that network traffic not directed to the proxy filters falls into a black hole.

Usenet and Other Parts of The Net—The Internet is far more than just the World Wide Web. Cyberspace includes Usenet, Electronic Mail, Chat and Instant Messaging, Bulletin Boards and multi-player gaming. And just like the web, the pornographers have a foothold in every corner of the net. Many filters deal only with web traffic and, while some email providers such as FamilyClick include profanity and obscenity filters for email and Usenet, other services available on the Internet are currently unfiltered like Instant Messaging.

Providers deal with these unfiltered services by not offering them at all, offering only a portion of the service or by issuing strong warnings to subscribers who choose to use these services. Usenet, for example, can be made semi-safe by screening out all but a few select newsgroups and by dropping all binaries. Electronic mail can be sanitized by comparing incoming messages against addresses of known spammers and pornographers and by scanning messages for telltale signs of porn and spam.

Staying Ahead of The Good Guys

As the masters of a billion-dollar enterprise, the porn web operators have every reason to want to defeat any technology that threatens to weaken their empire. For every step forward that the guys in the white hats take, the online porn industry takes two. Where once a simple word filter would suffice, it now takes sophisticated

software that can determine the context of a sentence or paragraph. Text messages that were at one time expressed in ASCII are now embedded in images that are impractical to scan. Porn site operators know who their enemies are and they are usually among the first to purchase and test new filters that come on the market. By the time a new filter gains widespread acceptance, the porn operators have developed methods of getting around the filters.

The technology that drives the Internet is advancing at breakneck speed and no industry is pushing this advancement more than the porn industry. Many of the first people to communicate with each other on the net talked about sex using a bulletin board devoted to erotic discussions. Pornographers were among the first to incorporate streaming video and pioneered the use of community software such as chat rooms and message boards. Each of these advancements has posed a new challenge to those that seek to identify and screen out unwanted material. The porn industry today is perfecting new technology and techniques that will make current filters obsolete. The porn industry is starting to incorporate 360-degree video and when digital scent technology is perfected, it will be the porn industry that first brings the sense of smell to your home computer. Filter writers that started with a simple list of four letter words now face the challenge of identifying and filtering different scents, sounds, textures, expressions and colors. The college graduate who wishes to push the state of the art would do well to seek a position in the online porn industry.

Because of the speed with which a porn master can drive traffic to a new site, web addresses that appear on blacklists are quickly replaced with new addresses. Many filters do not track the IP addresses of sites so porn operators often distribute addresses in the form http://209.25.138.4/new/open/open1.html. Such addresses contain no strings that might trigger a filter and the address normally leads to a site that will simply redirect the user to the existing, blocked site. These numeric sites are generally throwaway sites that are only intended to last for a few days. By the time these sites are listed by the major filters, new sites have replaced them.

Javascript Slamming is also frequently effective at defeating filters. Even if a filter blocks the first page, it may not block the rest. The porn operator who sends you through a dozen or more sites stands a good chance that at least one of those sites can pass through the filter.

Porn operators are also adept at hiding behind the first amendment. With cries of censorship, porn operators throw up many legal obstacles to the developers and providers of filtering services. Despite the obvious fact that participation in a filtered service is something that people elect, the porn operators have much support from free speech advocates who are quick to denounce this 'censorship' of the Internet. Many of these supporters maintain web sites such as www.peacefire.org that make available information on how to defeat various filters. Usenet groups such as alt.cracks contain information on how one might workaround the security features of various software packages including filters. Like all software, filters have flaws and the opponents of filtering are quick to point out that filters have mistakenly blocked sites such as the Quakers home page and the AIDS Memorial Quilt. They are usually not so quick to tell you when the filters are fixed.

Also in the name of free speech and privacy, web sites known as anonymizers have sprung up. These sites allow you to surf the web anonymously by accessing other sites on your behalf; acting as an intermediary between you and a filter. Most filters now block the anonymizers but new anonymous surfing sites are being launched about as fast as the filters can find them.

Even the best filters can't be expected to be 100% effective. Filters sometimes block sites that shouldn't be blocked. Likewise, the occasional inappropriate site sometimes slips through even the best filters. But most providers of filtered access are quick to investigate and correct any errors that are brought to their attention. Providers such as FamilyClick form a partnership with their subscribers; realizing that the most effective way to ensure safe access to the Internet is to work together. Subscribers are encouraged to suggest sites that should or should not be blocked and suggestions on how to improve the service are gladly accepted.

People who invest in the protection of a filter expect that filter to work 100% of the time. Unfortunately, that isn't currently possible. The online porn industry is able to deploy resources that the good guys can only dream about. The porn industry operates in an environment of cooperation and trust unheard of in other industries. While traditional technology companies zealously guard trade secrets, the porn industry willingly shares these tricks of the trade with each other.

Conclusions

Pornography is a part of society and probably always will be. But, away from cyberspace, one normally needs to seek it out in order to access it. Erotic magazines

and books exist but they are behind the counter. You need to ask for them. Pornographic videos exist and many video stores carry them. But they are in a back room; often protected by a locked door. Many cable television and satellite providers carry adult movies. But they are accessed via Pay-Per-View; they normally cost more than mainstream movies and they often require a PIN number to view. Your town may have a sex shop or X-rated theater but it's probably not next door or across the street. More than likely it is somewhere else in town along with all the other sex shops in a Red Light District. Although movies, television shows, video games and literature are becoming more and more suggestive, to access real porn you need to go out of your way to get it.

But not on the Internet. Away from the net, you normally need to look for porn. In cyberspace, it looks for you. On the net, pornography isn't behind the counter and it's not in a locked room. It isn't secured by a PIN number or access code and it's not on the other side of town. It's in your neighborhood, it's in your schools and it's across the street.

It's in your home.

Many families have brought filters into their homes, not to censor, but to protect their families from people and influences they would never allow through their front door. They rely on and expect these filters to work and protect them. The technological aggressiveness of the porn industry makes it very difficult to give families, that have opted to utilize filtering, a guaranteed safe Internet experience. Currently, technology is the only deterrent to accessing pornography on the Internet and it is always a step or two behind the latest techniques developed by the porn industry to drive traffic to their web sites. The role of FamilyClick and other providers of filtered access, is to provide the families, that have freely chosen filtered access, the safest possible experience while on the Internet.

Thank you for giving me the opportunity to discuss this important matter with you today. FamilyClick is prepared to work with the committee on this issue and I will gladly answer any questions you may have.

Mr. TAUZIN. Thank you, Ms. Stewart.

We will next hear from Janet LaRue, senior director of legal studies, Family Research Council, here in Washington, D.C. Ms. LaRue.

STATEMENT OF JANET M. LaRUE

Ms. LARUE. Thank you, Mr. Chairman, members of the subcommittee. Good morning. I am Janet LaRue and I am senior director of legal studies at the Family Research Council. Pornography law has been an area of expertise in my practice for many years.

As you know, obscenity is not protected by the Constitution because, by definition, it is patently offensive appeal to a prurient interest in sex and has no serious value. It is illegal to display or distribute to any person through any medium, including the Internet. The Supreme Court has reiterated that. It is the crass commercial exploitation of sex by a worldwide industry now estimated by Forbes magazine at $56 billion per year. Much of this is controlled by organized crime. This is an industry that exploits the basest nature of human beings, including those who are most vulnerable to addiction, especially children.

Minor children are no exception. If anyone doubts that, I would encourage you to visit the commercial pornography sites on the World Wide Web and see the plethora of free teaser images that are there, available for any child to view. In fact, I have with me today some photocopies of images that I just downloaded from the Internet, and Mr. Chairman, I would submit them for the record.

Mr. TAUZIN. The Chair will withhold on that request if you don't mind.

Ms. LARUE. These images include bestiality, mutilation, torture, excretory functions, orgies and other perversions. Internet pornog-

raphy is estimated by Forbes magazine at $1.5 million per year at this current time. According to Adult video News which is the online publication for the porn industry, "48 million unique hits on the adult Net daily." Forty-eight million daily. According to Nielsen net ratings, 17.5 million surfers visited porn sites from their homes in January, a 40 percent increase compared with 4 months earlier. Forty percent increase.

Researchers from Stanford and Duquesne University have now estimated that we have 200,000 individuals in this country that they define as cybersex compulsives, and I believe they have set the bar very high. To be a cybersex compulsive, one must visit a pornography Internet site at least, at least 11 hours per week. They said that this is a hidden public health hazard, exploding in part because very few are recognizing it as such or taking it seriously. Treating a new public health problem of this magnitude will place inestimable burdens on our health care system and unimaginable stress on adults, their families and society.

For several years, Family Research Council has been calling on the Department of Justice to begin an aggressive enforcement policy against major obscenity distributors. On October 28, 1999, I was one of several representatives of several profamily organizations who met with the head of the criminal division of the Department of Justice, Mr. James Robinson, and representatives from other Federal agencies who have responsibilities for obscenity investigations and prosecutions. Once again we voiced our concerns and complaints about the lack of prosecution. I personally provided Mr. Robinson with a stack of materials, photocopies of commercial porn sites that especially target teenagers. These hard-core images easily meet the definition of obscenity under Miller versus California.

The response from Mr. Robinson in his follow-up letter to our group was unacceptable and frustrating because nothing has changed.

In addition, the accessibility of hard-core porn on the Internet is turning America's public libraries into virtual peep shows open to children and funded by taxpayers. I have with me a publication recently released by the Family Research Council, called Dangerous Access, 2000 edition, uncovering Internet pornography in America's libraries. This is a result of Freedom of Information Act requests that were mailed to over 9,700 of America's public library systems, asking for any reports, complaints, or other memoranda having to do with patrons in public libraries accessing pornography. After 6 months of going through those reports and compiling the result, we have published it in this document. We show by libraries' own records over 2,000 incidents of patrons, including small children, accessing pornography; sex acts occurring in public libraries; sex crimes occurring in public libraries. We have mailed a courtesy copy to every Member of Congress, and I would offer a copy for submission into this record.

Mr. TAUZIN. The gentlelady again, we will withhold on that request, and we are asking counsel to advise us frankly, Ms. LaRue, as to what is the legality of introducing material into the record that may itself constitute obscenity, and realizing you want to make a point by showing us what you can download from the Inter-

net, but if you can withhold on those requests until we get an answer I would appreciate it.

Ms. LARUE. My point is to make the committee aware of the kinds of material we called to the attention of the Department of Justice that is rampant on the Internet, to which they said they would consider prosecution. As yet we have not heard of any.

Mr. TAUZIN. I think your report, without objection, will be introduced into the record. So ordered. I am simply asking that you withhold on the request. In fact, I would personally ask you not to make the request so we don't have the issue. I don't know the legality of putting in the record material that may in fact be obscene and having a record that may be duplicated or copied for the purposes of the public later on, as to whether or not we ourselves would be doing something which might violate the law. And I would frankly request that you not request us to introduce the earlier material into the record. Can I have that agreement perhaps?

Ms. LARUE. I would abide by your request. I would say that I did offer a similar stack of material to another House subcommittee, which was accepted, and I assume that——

Mr. TAUZIN. We may be able to do that. I would just simply ask you to withdraw it for the time being until we have a chance to get an answer for that from legal counsel. I thank you. You may proceed.

Ms. LARUE. Yes. Computerized cyberporn is a source of potential legal liability for the creation of a hostile work environment and specifically in violation of Title 7 of the Federal law. As a matter of fact, seven librarians in Minneapolis, Minnesota have recently filed a sexual harassment, hostile work environment complaint with the Equal Opportunity Commission. The complaint cites conditions in the library where sex offenders congregate 6-year-olds to view hard-core porn, men masturbate, and a porn surfer brandishes a knife when told to terminate his Internet access. These are conditions one would expect to find in a dirty bookstore, except for the presence of 6-year-olds viewing hard-core pornography.

Month after month for the past 7 years, Adult Video News has praised the Clinton Justice Department for not enforcing the Federal obscenity laws. The March issue states: "how likely is it, would you say, that we are going to enjoy the same benevolent neglect that the industry has enjoyed under Janet Reno? Regardless of who is elected, our fortunes are going to change."

I would close by asking the members of this subcommittee to consider that if a major drug cartel had a monthly publication in which they praised the Drug Enforcement Agency for not enforcing the Federal drug laws, how long would the people of this country or this Congress tolerate such conduct? I suggest that it would not be tolerated and especially for 7 years.

The Department of Justice refuses to enforce an entire body of the Federal Criminal Code that prohibits the trafficking in obscene materials. It must be called to account and be held responsible. Thank you.

[The prepared statement of Janet M. LaRue follows:]

PREPARED STATEMENT OF JANET M. LARUE, SENIOR DIRECTOR OF LEGAL STUDIES, FAMILY RESEARCH COUNCIL

Mr. Chairman, members of the Subcommittee, good morning. My name is Janet M. LaRue. I am senior director of legal studies for the Family Research Council (FRC) in Washington, D.C. Thank you for the opportunity to testify today regarding the problem of obscene material available on the Internet.

Pornography law has been my area of expertise for many years. I have lectured on the subject in numerous law enforcement conferences across the country, testified before state and local legislatures on pornography bills, and authored numerous appellate briefs that have been filed in the U.S. Supreme Court, federal circuit courts of appeal, and state appellate courts on various pornography law issues. The protection of children, families, and society in general from the serious harms of pornography, and especially obscene materials, is a top priority of FRC and of my department, in particular.

As you know, obscenity is not protected by the Constitution because, by definition, it is a patently offensive appeal to a prurient interest in sex and has no serious literary, artistic, political, or scientific value. It is illegal to display or distribute to any person, including adults. It is the crass commercial exploitation of sex by a worldwide industry now estimated at $56 billion dollars per year,[1] much of which is controlled by organized crime. This is an industry that exploits the lowest part of human nature and plays on those vulnerable to addiction in order to attract a new generation of customers. Minor children are no exception. Anyone who doubts that need only visit the commercial World Wide Web porn sites that flagrantly display scores of free teaser images of their product. These images include bestiality, mutilation, torture, excretory functions, orgies, and other perversions. I have copies of sample materials with me today that I offer for submission into the record. Internet pornography is estimated at $1.5 billion per year.[2] According to *Adult Video News Online,* there are "48 million unique hits on the adult Net daily."[3] "According to Nielsen NetRatings, 17.5 million surfers visited porn sites from their homes in January, a 40 percent increase compared with four months earlier."[4]

Researchers from Stanford and Duquesne University have estimated that 200,000 individuals fit the definition of "cybersex compulsive"-spending at least 11 hours a week visiting sexually oriented areas on the Internet. The Psychologists who conducted the research said: "This is a hidden public health hazard exploding, in part, because very few are recognizing it as such or taking it seriously."[5] Treating a new public health problem of this magnitude will place inestimable burdens on our health care system and unimaginable stress on addicts, their families and society.

In addition to the many other serious problems caused by the proliferation of hard-core pornography in our country, its accessibility via the Internet is turning America's public libraries into virtual "peep shows" open to children and funded by taxpayers. This is primarily due to failure of the Department of Justice (DOJ) to enforce federal obscenity laws.

FRC has been calling this problem to the attention of the DOJ for several years. On October 28, 1999, I was one of the representatives of pro-family organizations who met with the head of the criminal division of DOJ, James Robinson, and representatives from other federal agencies who have responsibility for obscenity investigations and prosecutions. Once again, we voiced our concerns and complaints about the lack of obscenity enforcement by DOJ. I personally provided Mr. Robinson with numerous photocopies of images that I downloaded free of charge from commercial pornography Web sites. These hard-core images easily meet the definition of obscenity under *Miller v. California,* 413 U.S. 15 (1973). The response from Mr. Robinson and his follow-up letter to our group was unacceptable and frustrating because nothing has changed.

FRC is especially concerned about the effect on America's public libraries caused by the lack of obscenity law enforcement. With the help of FRC, David Burt, a public librarian who shares our concerns, mailed more than 14,000 Freedom of Information Act requests to the nation's 9,767 public library systems, requesting copies of complaints, reports and other documentation of incidents involving patrons accessing pornography.

---

[1] Richard C. Morais, *Porn Goes Public,* Forbes, June 14, 1999.

[2] http://www.forbesfinder.com/forbessearch/search.asp?act.search=1&q1=porn+business&RD=DM&MT=porn+, visited April 10, 2000.

[3] http://www.avonline.com/200003/corecontents/cc0300—01.shtml, visited April 11, 2000.

[4] Brendan I. Koerner, *A Lust for Profits,* U.S. News & World Report, Mar. 27, 2000, at 36.

[5] Al Cooper, David L. Delmonico, Ron Burg, *Cybersex Users, Abusers, and Compulsives: New Findings and Implications,* Journal of Sexual Addiction & Compulsivity 25, 7:5-29, 2000.

A six-month investigation of the responses received uncovered more than 2,000 documented incidents of patrons, many of them children, accessing pornography, obscenity, and child pornography in the nation's public libraries. Many of the incidents were highly disturbing, as librarians witnessed adults instructing children in how to find pornography, adults trading child pornography, and both adults and minors engaging in public masturbation at Internet terminals. Analysis of computer logs from just three urban libraries revealed thousands of incidents that went unreported, indicating that the 2,062 incidents represent only a fraction of the total incidents nationwide. The total number of incidents each year nationwide is likely to be between 400,000 and 2 million. FRC has published the results of the investigation in a booklet titled *Dangerous Access 2000 Edition: Uncovering Internet Pornography in America's Libraries.* I offer a copy for submission into the record.

Dangerous Access, page 5

Incident Reports, Patron Complaints, and News Stories	Number
Child Accessing Pornography	472
Adult Accessing Pornography	962
Adult Exposing Children to Pornography	106
Adult Accessing Inappropriate Material	225
Attempted Molestation	5
Child Porn Being Accessed	41
Child Accidentally Viewing Pornography	26
Adult Accidentally Viewing Pornography	23
Child Accessing Inappropriate Material	41
Harassing Staff with Pornography	25
Pornography Left for Children	23
Pornography Left on Printer or Screen	113
Total Number of Incidents	**2,062**

Dangerous Access, p. 36.

Incidents included reports describing criminal conduct:

Crime	Number Documented	Number Reported to Police	Percent Reported to Police
Accessing Child Pornography	41	5	12
Accessing Obscenity	25	0	0
Exposing Children to Porn	106	0	0
Public masturbation/fondling	13	1	8
Total	**172**	**6**	**3.5**

Whether exposure occurs in a public library, school, nonprofit group, or business, workplace pornography and computerized "cyberporn" are a source of potential legal liability for those vested with management or control over the respective work environments. The viewing of pornography in public places creates an offensive, uncomfortable, and humiliating environment (in addition to unlawfully exposing or displaying such "harmful" material to minors). Pornography in the workplace can constitute, or be evidence of, sexual harassment in violation of state and federal civil rights laws and create or contribute to a hostile environment in violation of Title VII's general prohibition against sexual discrimination in employment practices.[6]

This month, seven Minneapolis librarians filed a complaint with the Equal Employment Opportunity Commission because of the hostile and offensive working environment caused by daily exposure to Internet porn. The complaint cites conditions in the library where sex offenders congregate; six-year-olds view hard-core porn; child porn is left on printers; men masturbate; and a porn surfer brandishes a knife.[7] These are conditions one would expect to find inside a dirty bookstore, except for the presence of six-year-olds.

[6] *See* 42 U.S.C. § 2000e-2; 29 CFR 1604.11; 18 U.S.C. § 242; 42 U.S.C. §§ 1981, 1982. *See Pornography, Equality, and a Discrimination-Free Workplace: A Comparative Perspective,* 106 HARVARD LAW REVIEW pp. 1075-92 (1993); *Robinson v. Jacksonville Shipyards,* 760 F. Supp. 1486 (M.D. Fla. 1991).

[7] Paul Levy, *Complaints filed over Web porn at Minneapolis Public Library; Librarians say they work in a hostile environment,* Minneapolis Star Tribune, May 4, 2000, at 1B.

Month after month for the past seven years, the trade publication of the porn industry, *Adult Video News Online,* has praised the Clinton Justice Department for not enforcing the federal obscenity laws. The March issue states, "How likely is it, would you say, that we are going to enjoy the same benevolent neglect that the industry has enjoyed under Janet Reno? Regardless of who is elected, our fortunes are going to change."[8]

Members of the Subcommittee, if a major drug cartel had a monthly publication that repeatedly praised the Drug Enforcement Agency for its "benevolent neglect" toward enforcing the federal drug laws, I don't believe this nation or Congress would have tolerated it, and certainly not for seven years. The Department of Justice refuses to enforce an entire section of the federal criminal code that prohibits the trafficking in obscene materials. It must be called to account and held responsible.

Thank you.

Mr. TAUZIN. Thank you very much, ma'am.

And our final witness on this panel, Mr. Joseph Burgin, of Cincinnati, Ohio, brings to us his personal story. Mr. Burgin.

STATEMENT OF JOSEPH W. BURGIN, JR.

Mr. BURGIN. Thank you. I am here today to represent what I believe to be millions of men whose minds are being held captive by electronic images. Each of us are experiencing consequences to varying degrees but each of us are being adversely affected. But more so than a representation of masses of people, I am here to represent my two sons and my daughter who experienced some crushing pain because of their father's involvement with pornography.

In my case, humanly speaking, I have lost everything that a man would hold onto to give himself meaning and perspective in life. Because of my involvement with pornography, I lost my marriage of 25 years. It also cost me the role of daddy, which I cherished, to my 9-year-old daughter. My involvement with pornography also cost me job opportunities and the career path of my calling and choice. In addition to those things, I have lost friends and trust and respect from many. The consequences that are measurable and tangible in my own life have been devastating enough. Through all of my legal proceedings I have lost some $100,000 in support obligation, retirement funds, et cetera, et cetera, all easily traced back upstream to my involvement with pornography.

So in addition to those measurable consequences, my involvement with pornography also affected me adversely emotionally. It thwarted and hindered the normal development of coping skills with life and an ability to manage my life on a day-to-day basis. Instead of knowing how to do that, I was simply turned to the sedating effect that I could find from online pornography.

As a man in mid-forties, I am now having to go back and relearn those things to have any hope of any future that is any semblance of normal relationships.

Through an awful lot of professional counseling and hours upon hours of attendance at support groups and with accountability partners, I have been able to find freedom from pornography.

But I can't talk about the consequences before you today in the past tense. Because of my involvement with pornography, I feel I am scarred, I am handicapped, I will move into my future with a limp. I will always be affected because of my years of involvement

[8] http://adultvideonews.com/legal/leg0300.html, visited April 11, 2000.

with it. The moment any forward progress stops, then my regression begins.

So I am here today to make an appeal to do anything or everything that is conceivable to thwart or hinder the development of this industry. In my own personal life it has brought devastating consequences, and as my oldest son Josh said, tell them about it, Dad; it has gotten out of hand, it has got to stop. So my family for one, we are fed up with the industry.

Thank you.

[The prepared statement of Joseph W. Burgin, Jr. follows:]

PREPARED STATEMENT OF JOSEPH W. BURGIN, JR.

I am 46 years old. I am divorced after being married 25 years. My oldest son is a junior in college. My middle child lives with me and is a junior in high school. I also have a 9-year-old daughter who lives with her mom. I hold a Bachelor of Arts and Master of Arts degree. For 20+ years I provided leadership and management for nonprofit organizations in Ohio and Alabama. A major publishing company currently employs me as a regional manager.

I consider myself a sex addict with Internet pornography being my primary means of acting out. I feel I have been a sex addict for more than thirty years. I have been in recovery for about two years. In my active days of addiction I felt my self-esteem was very low. I feel that in my addiction I struggled with depression. I consider myself in recovery from sex addiction with no relapses for a year and two months. My religious beliefs are protestant. The Internet was an active part of my addiction. I have used Internet photos and videos for my addiction. The Internet reactivated my addiction that was inactive for years. I feel the Internet took my acting out to a different level because of its ease of access. I believe my sexual orientation is heterosexual. I acted out in my addiction only with myself. All of my sexual fantasies in my addiction were about women I did not know. The type of porn I would use was mostly hard-core (sex acts depicted). In my marriage I had no affairs.

Since adolescence, I did a masterful job of concealing my struggle with sexual addictions and pornography. My own self-hatred, other personal handicaps and as well as relational weaknesses made me a prime target for pornography. Internet pornography was extremely easy to access and hide. I deal with men regularly who are caught in this trap because of the ease with which it can be accessed. I was sought out as a customer through banner adds, Spam, unsolicited email attachments, etc.

The day of reckoning came in my life as a torpedo hit me with a full broadside blow and my life sank. After going through an unwanted job change along with the death of my father and other personal issues, I returned to an old friend for relief—pornography. For a few days the sedating effect from hour after hour immersion in pornography numbed me out and I didn't feel any pain. But my life-long hidden addiction soon came to light and my sons and subsequently my wife discovered my darkest secret. As a result, my addictions cost me: my marriage; the role I cherished as daddy; job opportunities in the field of my calling and choice; legal problems resulting in over $100,000 of fees, retirement income, and support obligations; significant financial difficulties; loss of friendships; loss of credibility and trust in the eyes of some; etc. I've felt the stinging backhanded blow of professional peers and the abandonment of many alleged friends. The consequences of pornography affected me emotionally with a deep and permeating sense of shame and guilt. I've struggled with loneliness and feelings of abandonment, rejection and betrayal. The pain at times has been crushing. My anger toward pornography is intense—it cost me all this and more while the pornographers make billions.

In addition to the external measurable consequences, addiction to pornography also affected me emotionally and thwarted my development of appropriate relational and coping skills. I feel it caused me to objectify women seeing them as nothing more than a means to satisfy my desires. I grew less satisfied with my wife's affection, physical appearance, sexual curiosity, and sexual performance proper. Sex without emotional involvement became increasingly important. It created feelings of power and control and led to me becoming a manipulative and controlling person to those closest to me.

Thousand of dollars, hours of guidance by a professional Christian counselor, hours in support groups and with accountability partners resulted in health and healing and freedom. But the road is uphill and difficult. It is easily the hardest thing I have ever done in my life to find freedom from pornography. I feel my relapse will begin when active recovery stops. There is no standing still, taking a

breather, or pausing for a rest. When the forward motion ends, the backward motion starts. A recovering addict likened it to a tide: It is either coming in or going out, and it never stands still.

I'm glad the Lord I serve is the Lord of the Mulligan. My God has helped me to get up off the ground and get back into the game. "Hey kiddo, let's take a Mulligan on that one, okay, and start again. But this time let's don't include pornography in the game?"

Centuries ago, John Chrysostom wrote, "*The danger is not that we should fall . . . but that we should remain on the ground*." At times over the last few years I have thought there is no tomorrow because of pornography, but the sun has been coming up each day. I've been able to come to a better place but not until I found freedom from pornography.

Sustained by God's unmerited favor, Jody Burgin.

Mr. TAUZIN. Thank you very much, Mr. Burgin.

The Chair will recognize members in order for 5 minutes. Let me begin by asking, I guess, the legal side of the equation. We are told it is impossible, difficult or legally indefensible to bring an obscenity case on the Internet because of the concern that the Miller test by the Supreme Court does have a community standard feature: that it, one, requires on a national test the material be prurient, appeal to the prurient interest; second, that it is patently offensive, which is also a national test; but the third test which is based on a community standard is that it has no artistic, political, scientific or literary value based upon those community standards.

Now, what is different about the Internet in regard to enforcing the 3-point Miller test? Would anyone like to handle that?

Mr. FLORES. Mr. Chairman, what I would say is that first of all, the test, what we call the LAPS test, literary, artistic, political and scientific test, is actually judged by the reasonable person, so that is much more akin to a national standard which should not really put anybody at any substantial distress. And let me just say that the Justice Department, if I saw an accurate copy of the deputy assistant's testimony, is going to talk to you about the Thomas case. The Thomas case was prosecuted before the 1996 amendment. That was a specific argument that was raised by the defendants and rejected by the court of appeals, and the Supreme Court refused to accept certiorari, so that case died right there.

Mr. TAUZIN. Let me ask you in the offline world, if a violator of the Nation's obscenity laws were to mail or send in a package with UPS obscene material to a site elsewhere in the country, would not the obscenity laws still provide a vehicle for prosecution either at the site where the material was mailed or at the site where it was received, based upon the community standards test?

Mr. FLORES. That is correct, Mr. Chairman.

Mr. TAUZIN. I guess what I am asking, what is different on the Internet, where a potential violator who wishes to send obscene material over the phone wires, over a cable system, over a satellite structure, over terrestrial wireless structure, sends it from a point of location to another point where it is being viewed or in some way copied, what have you, in a way that does violate the obscenity laws of that locality—could not a prosecution be made both at the point where the material is first sent over those systems of communications, over the Internet or over a phone line, or at the point where it is being distributed in a community which has community standards, that would clearly define that material as obscene?

Mr. FLORES. That is right, Mr. Chairman. Not only that, but that is what guarantees that our communities are going to have freedom, because if we had a national standard, then every community would be forced to abide by one separate standard. This is what allows Californians per se to have a different community standard and those in Memphis or Maine or anywhere else to have a separate one. And the fact that it is on the Internet, I mean folks who use the Internet now should know at least one thing; and that is, once they release that material, they know that it goes into every community. In fact, that is what they are banking on.

Mr. TAUZIN. In fact, the fact that some of these companies are actually going public, as you point out, going into IPOs and raising incredible amounts of money, would that be occurring on Wall Street absent this—what Ms. LaRue called this "benevolent neglect" in terms of prosecuting these companies for distributing obscene material?

Ms. LARUE. I don't believe so. In fact, I believe that Wall Street and others assume that because this material is rampant on the Internet, that these people are providing a legal product. Certainly we wouldn't have the promotion by legitimate business of an enterprise that is constantly producing material that violates Federal law.

Mr. TAUZIN. In regard to the laws here, can the State authorities equally process these laws and bring cases against companies that are located in, let us say California, that is going forward with an IPO to distribute this material around the country and around the world?

Mr. FLORES. There is certainly a sphere of control that States have in this area but they certainly don't have the tools nor do they have the ability, because the Justice Department has jurisdiction over the entire United States. They don't have the jurisdictional problems and disputes, and they have a unified Federal system. So this is what makes the Federal Government the best place to spend the limited money that is available to do this, but because of the abdication, many States and localities are having to take this battle on even against traditional pornographers because that is the only people who do it.

Mr. TAUZIN. You call it an abdication. You call it benign neglect. I guess I want to ask the right question. Have cases been brought to Justice and Justice refused to prosecute them, or is Justice in your opinion just not looking to make a case? What is the story?

Mr. FLORES. Mr. Chairman, I know that when we met in October, as Ms. LaRue indicated, I brought to their specific attention the fact that Amateur Action, the subject of the Thomas case, was back in action and this time they were selling on the Internet movies which depicted amputees engaging in different types of penetration. This material wasn't education. It wasn't scientific. It wasn't offered as a way to teach those who are disabled. This is incredibly prurient and patently offensive material. I brought it to their attention and clearly what came out of that was that simply they have a different set of priorities.

Mr. TAUZIN. Ms. LaRue, you had your hand up.

Ms. LARUE. Yes, I can attest to that. And also as to your question about States enforcing obscenity laws on the Internet, I per-

sonally assisted the pornography section of the Los Angeles Police Department to prosecute a computer bulletin board service operating in California. They got a conviction in that case. And by the way, the same type of argument was raised about community standards in that case, and I drafted the legal memo that the court accepted, and that argument lost, just as it did in the Thomas case to which Mr. Flores referred.

Mr. TAUZIN. Thank you, Ms. LaRue. The Chair recognizes the gentleman from Ohio, Mr. Sawyer, for a round of questions.

Mr. SAWYER. Thank you, Mr. Chairman, and let me thank all of our witnesses for your testimony today. It has been illuminating, and, Mr. Burgin, in some cases just tragic.

We find ourselves dealing not only with questions of the situs of prosecutions or origination of materials that all of us would find offensive when we are talking about prosecutions within the United States under U.S. law.

Have any of you given thought to the problems that arise with sites that originate in the United States but which actually transfer materials outside the United States; or the reverse, where sites are generated outside the United States and sending materials in? Do you have thoughts on how we address that?

Mr. FLORES. Mr. Sawyer, I would direct you to page 5 of my testimony. I just note that on March 9 of this year, deputy assistant Attorney General Kevin Di Gregory took justifiable pleasure in announcing that the week before his testimony a jury in Federal district court in New York found Jay Cohen, owner of an Internet gambling site in Antigua, guilty of violating Title 18, Section 1084, a statute that makes it illegal for a betting or wagering business to use a wire communication facility to transmit bets or wagers in interstate or foreign commerce.

Under the same theory that the Justice Department used to obtain the gambling conviction, there's no question that they would have the ability to do it. In fact there are cases, these deal with child pornography, which were prosecuted during the time that I was at the Justice Department, where foreign distribution, as soon as it went into the mailbox, they were able to initiate the prosecution because it was destined to come back to the United States. What the courts require is a substantial connection to the United States. So the court has oftentimes said that the only way to address these issues, really, is globally. So the Justice Department, I believe, is in the premier spot to really take some effective action.

Is it going to be perfect? I don't think so, but we don't ask that of any other area of law enforcement, and so I think that would be an inappropriate question for the Justice Department, or a level of success that they would require from this area they don't require from anywhere else. And we do drug prosecutions all over the globe, we do fraud prosecutions, copyright prosecutions. I mean, we are a very aggressive global litigator in every other area.

Mr. SAWYER. Let me ask about problems that are perhaps unique to the Internet. We have talked in a number of arenas about the problems of mirroring, where one site transmits another. Who is guilty in a circumstance like that, or does everybody who touches digital pornography become guilty or potentially guilty of the kinds of crimes that you would like to see prosecuted?

Mr. FLORES. With respect to that question, I guess I would, if I were sitting back at Justice, the way I would answer that question would be to take a look, first of all, to see whether or not the major players really are hidden from view in that way, because the reality is that there are, you know, tens of thousands of sites out there, but they are not owned by tens of thousands of discrete companies and individuals. And I think very quick research by the FBI, which is very capable, as well as my former colleagues at the Department, they could easily identify the top 20 or 30 companies. Many of them operate out in the open with a real office, real business records. They have got those servers here in the United States as well as overseas.

And so as we did when we started this fight in the late eighties, early nineties, what we have to do really is pick out the best targets. We do have limited resources. I don't think the mirroring problem would present at all an issue, either investigatively or legally, to prosecution of proper targets.

Mr. SAWYER. Finally, very quickly, as technologies merge, do you see a need to treat television and the Internet differently because of the nature of the medium or simply recognize that these are pornography and obscenity laws that need to be enforced regardless of the medium through which they are transmitted?

Ms. LARUE. That is certainly the approach that we would advocate. It also is what the Supreme Court has made clear, again in the Reno versus ACLU case, that obscenity distribution is illegal through any medium and the law applies to any medium.

Mr. SAWYER. Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman. The Chair recognizes the gentleman from Oklahoma, Mr. Largent, for a round of questions.

Mr. LARGENT. Thank you, Mr. Chairman. Mr. Flores, I would like to ask you, if I could, a few questions. We have had the Attorney General up on the Hill before various committees. A number of my colleagues have questioned her about this specific issue, about the lack of prosecution on obscenity cases, and when pressed for answer she would begin talking about the prosecution rates on child pornography and stalking; basically not addressing the real question, which is the obscenity issue, which is the focus for this committee hearing. And I would like you maybe to just give us a 2-minute primer on the difference between child pornography and stalking and obscenity cases, which is what we are trying to address here in this hearing today.

Mr. FLORES. Well, beginning first with probably the easiest, child pornography, in 1982 the Supreme Court, in a case we refer to as the Ferber decision, removed the whole area of sexually explicit material dealing with children. They took it out of the obscenity framework, so that it was no longer necessary for a prosecutor to prove that the material lacked value. In fact, Justice O'Connor in her concurring opinion noted that it really didn't make a difference to the child who was sexually exploited whether the material had value, and so if you had an Ansel Adams-quality photograph, that child is still being sexually abused. And for that reason, child pornography stands separate and apart as a type of material which is illegal. And recently the Congress took the last step in closing out

the last loophole, which is to simply say that all possession of child pornography, even one item, is a Federal violation.

Child stalking is a growing problem, and that deals with people who are out there seeking children for the purposes of sexual activity. This is not a new problem, but it is growing at a phenomenal rate, to the point where I was at a briefing that was held by Congressman Frank's office last year, where the FBI let us know that for all intents and purposes, they were now really focusing solely on child stalking, it had become such a big problem, and that with the exception of very significant child pornography cases, they were being forced to really just address that issue.

Obscenity, however, captures a broad set of materials and it is a term of art, a legal term of art, so that no lawyer should ever be confusing child pornography with obscenity, because obscenity is that material which passes a 3-part test. The first two prongs of that test are judged by contemporary community standards. The third is judged by the reasonable person test, and so it is not confusing. In fact, in a 3-year period, as I said I think earlier, we had over 120 convictions against no losses, as I recall, and there were fines and forfeitures of over $21 million in that period of time.

So the pornography industry certainly understands what we are talking about because, as a result of that effort, they stopped sending out, for the most part, unsolicited sexually oriented advertisements which today on the Internet is spam. They stopped carrying the most revolting material, primarily real sadomasochism and bathroom-related sex, and they stopped sending material entirely into certain communities where the community standard was very well-known.

So the term "obscenity" is also known extremely well to the ACLU and to litigants in the first amendment context, because in the CDA case, in the COPA case, they have not even begun to challenge whether or not those laws apply to the Internet.

Mr. LARGENT. So what I hear you saying is that the 3-prong test that was established in 1973 is just as applicable to the Internet as it is to any porn shop that we traditionally think of back in the seventies or the eighties. The Internet really has had no effect on the legal term of art, the definition, the execution, prosecution of the law that we had prior to the Internet?

Mr. FLORES. That is correct.

Mr. LARGENT. Okay. Ms. LaRue, I know that part of your testimony you talked about the meeting that you had in October with the Department of Justice. It is my understanding that at that meeting that you submitted some specific porn sites to the Department of Justice. What was their response in regards to those specific porn sites?

Ms. LARUE. Well, in both the meeting and the follow-up letter, Mr. Robinson said they found the suggestion that they enforce that provision of COPA—which makes it illegal to distribute obscene material to minors—be applied to the sites that I suggested. And he said he found that interesting and that they would consider it.

Mr. LARGENT. But the distribution of obscene material to anybody, adult or child, is illegal under current law; is that correct?

Ms. LARUE. Absolutely. But under COPA, Child Online Protection act, there was a provision added to the Federal code that

brings an enhanced penalty for anyone who knowingly distributes it to a minor.

Mr. LARGENT. So the law got better?

Ms. LARUE. Yes.

Mr. LARGENT. Not worse.

Ms. LARUE. Yes; doubled the penalty if you distribute to a minor under the age of 16. And there is currently a bill pending by Mr. Tancredo that would increase that to under 18.

If I might add to your comment about child stalking and child pornography, while no one here on this panel, I know, thinks that those aren't serious offenses, aren't we focusing on lesser—if you look at what has happened in New York City at the reduction of the crime rate, murder dropped 50 percent not because New York police suddenly started enforcing the murder statute they always had. It is because they started enforcing the statutes against lesser crimes because the principle is it flips upward. If you send out the message that obscenity will not be tolerated in the United States, the pedophiles will get the message that they better not have their child pornography up there because certainly that isn't going to be tolerated either.

And by the way, when it comes to child stalking, the effective tool in the hands of a pedophile is to use adult obscenity to desensitize children and to educate them into what the pedophile wants. So when we are asking that the obscenity laws be enforced, we truly believe that if it is done, that these other crimes will take care of themselves.

Mr. LARGENT. I yield back, Mr. Chairman.

Mr. TAUZIN. The Chair recognizes the gentleman from Texas, Mr. Green, for a round of questions.

Mr. GREEN. Thank you, Mr. Chairman. Mr. Flores, what years were you at the Justice Department?

Mr. FLORES. 1989 to 1997.

Mr. GREEN. Okay. So you were there during the beginning of the explosion of the Internet in 1997?

Mr. FLORES. Yes, sir.

Mr. GREEN. It started, I guess, even after I was elected to Congress in 1993, still people didn't know what Internet was back then.

I want to commend you on your statement on page 7 where it says, "Our Constitution protects speech but it does not protect obscenity," and I agree. We—in Congress we have tried for many years to pass laws that the Federal courts keep explaining to us that there is a difference between obscenity and pornography, and we can prohibit obscenity, but we have trouble prohibiting pornography to adults.

Most recently Congress passed the Child Online Protection Act and the President signed it in October 1998, a Federal judge in Philadelphia then immediately issued a preliminary injunction, and the Justice Department has announced they are going to appeal that ruling. Is there any update in status? That was in April of last year.

Mr. FLORES. We are waiting for a decision in the Third Circuit.

Mr. GREEN. I guess my concern is generally that testimony—is that the Justice Department is not prosecuting as aggressively as

they should be and aggressively as they did while you were there, and I know that is important to me because I want to see it happen. I also know that you know we pass laws and oftentimes the courts have a different interpretation than we do as Members of Congress. And I also agree that the legal definition of pornography and obscenity shouldn't be changed or it shouldn't matter what the medium is, whether it is the mail, the TV or the Internet. And it may be a little more difficult, but as you said in your testimony, you can prosecute even offshore facilities by attaching the assets here in our country, and we do that in lots of cases, both civilly and criminally.

Ms. LaRue, one of the questions when you talked about the availability of the Internet in public libraries, I agree that if I was sitting on a city council I would not want my Internet capability in public libraries to have access to that type of material, and put a filter on it. I don't know if Congress can make that decision for the City of Houston or City of Philadelphia. I wouldn't want it in the libraries any more than I would want it in our committee records.

I notice you place significant emphasis on Internet availability in libraries, and I am unclear. Should we not have Internet capabilities in libraries without filters, or should we just encourage the filters being on it in our public libraries?

Ms. LARUE. We would encourage the Department of Justice to enforce the Federal obscenity laws, and we wouldn't have the problem that we have in public libraries.

Mr. GREEN. Well, again, the availability of the Internet in a public library, I can walk in, whether it is myself or my children who are no longer minors, or my children who may have been minors at one time, and maybe our fight should not only be on the Federal level but also on the local level to say at a public library, I would hesitate to have my tax dollars being spent for access to that kind of information. So, again, I think it could be a 2-pronged effort and ensure the overall prosecution because—whether it is a public library or somebody's home computer. But do you believe libraries should have access to the Internet?

Ms. LARUE. I have no objection to that at all. My objection is to the bringing in of illegal material through taxpayer-funded government facilities, and we wouldn't be having the discussion here today, I don't believe, if the Department of Justice were enforcing the law.

Mr. GREEN. Well, again, the courts have said that, you know, again whatever medium, whether it is Internet, mail or television, that pornography, we have a hard time defining that, and so the pornography may still be available but it is not obscene, at least under the definition, but that would still be available in the public libraries.

Ms. LARUE. We are advocating the prosecution of hard-core pornography that the court has clearly given us examples would meet the definition in Miller versus California.

Mr. GREEN. Of obscenity.

Ms. LARUE. Yes. There is also State law available that prohibits the dissemination of material harmful to minors, and the Supreme Court in Reno versus ACLU took note of those State laws that are applicable as well.

Mr. LAASER. Mr. Green, I would just point out that any of us who are therapists in this field have seen cases of teenagers, 11, 12, even 13-year-old children who have gone and accessed pornography in public libraries. I personally am treating a case of a child that accessed sadomasochistic activity at the public library. So it is available there, and they don't need to be that computer-sophisticated to get at it.

Mr. GREEN. I guess my concern is that we should—again, we try to define what we don't want children to see, and of course the Supreme Court has said adults can see it. How do we differentiate between whether it is a child, 12-year-old or 13-year-old sitting in that terminal, or adult? That is a local decision.

Again, if I was sitting on a city council, I would say well, wait a minute, I am so fearful of my child seeing it, I would filter it out for anyone in the public libraries, and I don't know if they would allow us to prohibit that.

Mr. TAUZIN. The gentleman's time has expired. Anyone wish to respond?

Mr. FLORES. Just, Mr. Green, what I would say is that everyone is struggling with this issue. I know State government officials, library officials, who are struggling. The people who apparently are missing from the discussion, missing from the effort, is the Justice Department and that is a very big absence.

Mr. TAUZIN. The gentleman's time has expired. The Chair recognizes the Vice Chairman of the committee, Mr. Oxley, for a round of questions.

Mr. OXLEY. Thank you, Mr. Chairman. As the author of the Child Online Protection act, I take some particular interest in this issue, and we are obviously waiting for the Third Circuit decision, although I must admit I was somewhat taken aback by the Supreme Court decision announced yesterday regarding cable, which was a relatively minor effort to try to get some handle on that issue. And we hope that the decision ultimately by the Third Circuit or ultimately the Supreme Court has a different ending, but in the meantime I guess we learned that we need to rely on existing laws for our prosecution, and clearly prosecution equals deterrence.

Ms. LaRue made a good point about New York City. All you have to do is visit Times Square today and compare it to when I lived in New York back in the late sixties, early seventies, what a huge change that has meant to just that area but, as well, the entire city. So, really, enforcement does provide a great deterrent to that kind of behavior.

The unfortunate fact is that the prosecutions have declined significantly. As a matter of fact, Mr. Flores, do you know of any obscenity prosecutions in 1999 by the Department of Justice? We couldn't find any.

Mr. FLORES. Well, Mr. Oxley, there are a few obscenity cases that were done, but none in the way I think that you are asking the question. There have been zero cases done involving a Web site or anyone doing business over the Internet. There have been some people who have used the Internet to advertise, but they are basically running a mail order business. I think there is one case there, and then there may have been a few others.

Oftentimes what you will see in child pornography cases is that they will include obscenity charges, and because the obscenity section is 1460 and following, as compared to the child pornography section which is 2251 and following, the obscenity charges lead off; and in the recordkeeping systems of the Justice Department, oftentimes it is the top charge, the lead charge that is recorded. And so unless you actually get the name and docket number and then actually look to see what the charges are that are brought, you cannot in fact identify what is going on.

My best information, from talking to former colleagues and from folks across the country, is that there maybe have been a handful of cases done in the past 2 or 3 years that are really obscenity cases, and many of those stem from cases that were begun in 1993 and 1994.

Mr. OXLEY. Well, I want to personally thank you for helping us on COPA and all the work that your center did. Clearly we made enormous progress but there is a lot more to do.

I was struck by a quote from a New York Times article in 1986. The article was entitled "X-rated Industry in a Slump. The pornographic industry's plight is due partly to legal challenges. With little help from the Reagan administration, an unlikely alliance of conservatives and feminists has persuaded many retailers to stop carrying adult magazines and videos, said Martin Turkle, one of the largest distributors of adult videos in the country. Next year is going to be the roughest year in the history of the industry," and indeed it was. The sales of adult videos at the wholesale level dropped from $450 million to $386 million. That is compared to $3.9 billion, by the way, in 1996 which I am sure that those numbers have increased dramatically.

And last, from the Los Angeles Daily News article, this says, "Before Clinton took office, Los Angeles police were deputized by the Federal Government so they could help prosecutors conduct monthly raids on Valley pornographers. Under Clinton there have been no raids, said Los Angeles Police Lieutenant Ken Seibert. Seibert said adult obscenity enforcement by the Federal Government is practically nonexistent since the administration changed," end quote.

Well, indeed, we are really in a trap here because if we have to rely on existing laws until COPA is determined to be constitutional—and there is some question now with the recent 5-4 Supreme Court decision—so we are based in a situation where we have to rely on existing laws, and we rely very heavily on the Justice Department to carry out that law. And it is just not being done, and that is what the purpose of this hearing is about.

I commend my friend from Oklahoma for pursuing this so doggedly, because it does point out, I think, that deterrence comes about because of strong law enforcement, and just the opposite happens when you don't, and we have seen those numbers increase dramatically.

I was told during the COPA hearings, and I wonder if anybody can bear this out, that there are over 10,000 commercial pornographic Web sites out there. Is that accurate?

Ms. LARUE. That is too low. The estimate is more like 40- to 100,000 sites.

Mr. OXLEY. Just domestically?

Ms. LARUE. Yes.

Mr. OXLEY. That is a frightening figure. It gives you an indication about how the pornographic industry really has gotten the upper hand in this whole equation.

Thank you, Mr. Chairman.

Mr. TAUZIN. The Chair recognizes the gentleman from Florida, Mr. Stearns, for a round of questions.

Mr. STEARNS. Thank you, Mr. Chairman, and I want to thank you for having this hearing and I want to thank my colleague from Oklahoma for his hard work on this.

Mr. Burgin, I am going to compliment you for your personal courage. The witnesses we have today are here to testify and the witnesses from the Department of Justice are here to testify, but they don't have the personal courage and strength that you have, and I want to compliment you for it and thank you for it, and I think everybody who has a family should certainly understand what you have been through.

I think the concern I have—Mr. Largent has given me a chart here to show, you know, the difference between obscenity and indecency and so forth. Because the Internet is so pervasive, did you find this addiction, this sedating effect because of its availability through the Internet, did you have this feeling that because it is in—I guess what I am asking is, did this start before the Internet or was the Internet the start of this whole process? Because you can go into the magazine stores, you can see it in television. As you know, here in Virginia, in Metropolitan Washington, Maryland, the cable TVs have scrambled the pornography, but the scrambling—the voice is still available and scrambling is not complete. So I mean, I think we have to pass laws, but I am concerned a little bit about how this came about, I guess, and that is my question.

Mr. BURGIN. Okay. My own personal experience predated the Internet. My father introduced me to pornography during my adolescent years. I went underground for many years on and off dealing with the issue. What happened in the eighties when I discovered the Internet is that my addiction accelerated. It took off and went to a completely different level, mainly because of its ease of access and was so easy for me to hide and to mask from my own family, from my wife, from my children. So the Internet for me provided ready access, and it caused my addiction with pornography to accelerate to a different level.

Mr. STEARNS. Dr. Laaser, I would like you to participate because I was going to ask you, in the patients you have treated, how many would you classify as addicted to obscene material, which is illegal, as opposed to those who are addicted to legal pornography? That is the next question.

Mr. LAASER. I just wanted to commend you about your question about etiology, about where does it start. And my answer to that would be that we are seeing today a population of addicts that might not otherwise become addicted because of the easy access to the Internet. In other words, my clinical colleagues are beginning to speculate that, you know, there are a whole set of people whose prohibitions would be such that would keep them from going to a

bookstore, whereas the access on the Internet is allowing them to get in and get addicted.

So there is, like Bill W. of Alcoholics Anonymous would call a new level of low bottom of sexoholics out there, low bottom drunks getting addicted that wouldn't have been. I just wanted to say that even though Mr. Burgin represents a history of pornography before the Internet, we now today have an epidemic of sexual addicts who started on the Internet that might not otherwise be addicted.

In terms of your question, you want me to go ahead and respond?

Mr. STEARNS. Sure.

Mr. LAASER. The percentage would be—it depends a lot on how you define obscene. I would say that in my definition of obscenity, would be a lot lower, or however you define it, in terms of I think there are magazines available at the airport, where I will be later this afternoon, that are obscene. So you know, virtually 99 percent of the material that is available on these Web sites in my estimation is obscene. I bring a certain moral perspective to that that all might not share. So in that case, 100 percent of my clients are addicted to obscene material.

The percentage of those that might get into the violent, those are all people that have, you know, emotional disorders that are underlying the addiction that need to be present, but what we are seeing is that more people are escalating to higher levels of addiction today than would have been the case just 10 years ago.

Mr. STEARNS. And now they are probably on a 56K modem.

Mr. LAASER. That's right.

Mr. STEARNS. But wait until we have broadband in which we have instant video and everything that goes with it, and eventually the high definition television. So what we are talking as a beginning stage here is if we think we have a problem now, once we get broadband.

Mr. LAASER. All right. Today, with virtual reality available, the prostitutes, the world's oldest profession, have been certainly creative. You can access prostitution on the Internet. As I say in my written testimony, I had a client this February who spent $85,000 on prostitution on the Internet. In other words, clicked in visual images being projected because the prostitute had a camera focused on herself. Those kinds of sites are available today all over the Internet for credit card moneys. You can pay your $2- or $300 at a shot.

So as computer technology improves and virtual reality improves, we are going to have interactive prostitution exchange. So I would commend this committee to get on top of this now because it is definitely getting worse.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. TAUZIN. The Chair recognizes the gentleman from Maryland, Mr. Ehrlich, for a round of questions.

Mr. EHRLICH. Doctor, I worked with these issues in the State legislature, particularly pedophiles and pedophilia. Would you care to comment with respect to what you just talked about, the unlimited—or what Mr. Stearns talked about—the unlimited access that we are talking about here with respect to studies that you are familiar with concerning organized pedophiles? And I know there are actually groups out there that march, that God knows will probably

apply for 501(c) status sometime. This is a very serious concern. It kind of gets lost sometimes in the course of this debate.

Would you give me your knowledge with respect to how this unlimited access problem has impacted numbers of pedophiles and organization thereof?

Mr. LAASER. Obviously, we are dealing with a population that is very secretive so academic research into the increase of the number of pedophiles has been rather limited, but I would say that all of my colleagues, including those who have written in a recent journal devoted to the issue of Internet pornography, are estimating that we are seeing a dramatic rise in pedophilish activities.

One of the rituals that your average pedophile will use is to show a child images of pornography, so that what we are seeing today is that the pedophiles who are generally hiding out in the chat rooms, disguised in a variety of forms, are engaging the trust level of the child. And then they are able now electronically to transmit images either of fairly soft stuff to begin with, again to gauge the trust, but then of themselves and other kinds of activities.

The easy accessibility of this, we believe, is increasing the numbers of pedophiles and certainly increasing the number of kids that are at risk to this.

Mr. EHRLICH. The empirical data I am familiar with reflects the fact that pedophiles, almost to a person, were abused as children.

Mr. LAASER. That is right.

Mr. EHRLICH. And of course what you are talking about plays into that as well.

Mr. LAASER. Your average pedophile was abused as a child, and the research would indicate that your average pedophile will offend against a child within a 1-year variance of the year at which they were abused. So that if a child was sexually abused at age 5, a pedophile's victims will normally be between the ages of 4 to 6. So that, yes, what you are calling is the—it is kind of what we refer to as a trauma bond; in other words, a victim becomes a victimizer. That is not a universal principle, but certainly your average pedophile today is an abuse victim.

Mr. EHRLICH. Your average pedophile, I guess the profile is such that you are not talking about one instance, you are talking about multiple offenses?

Mr. LAASER. No. Your average pedophile has at least 80 victims by the age of 35.

Mr. EHRLICH. To anybody on the panel, with respect to some of the sites that you are familiar with, how many are out there dedicated to the whole problem of child sex, pedophiliacs, et cetera?

Ms. LARUE. They certainly advertise the material as appeals to pedophiles because it refers to teen sex, barely legal, little girls, Lolita, all of the kinds of terms that would be meaningful to a pedophile looking for material. And so you see individuals where, even if you cannot be certain that they are under the age of 18, they are portrayed in that way, they are advertised in that way, and they are engaging in all kinds of hard-core sex acts.

Mr. LAASER. I would confirm the fact that we are seeing an epidemic of disguised child pornography. In other words, the models, you know, there is a fine print that says that the models are 18, but they appear to be 12 or 13. I would even say—and I am not

going to mention the magazine—but there is a cover of a recent magazine this month in which the model on the cover would appear to me to be 13 or 14.

So I mean, this is affecting us culture-wide, but on the Internet, particularly from some of the foreign Web sites, we are having a lot of direct stuff coming. But if you go into any bookstore today, you will see magazines like the Barely Legal magazine, Just 18, things of that nature. There is an epidemic rise in interest in this.

And, by the way, my clinical colleagues would want me to say that pedophilia is technically sexual interest in a child 12 and under. What we are talking about here with this teenage sexuality is 18 and under, and we refer to that as hebephelia, but it is a rampant problem and, again to say it for the 10th time, growing in epidemic proportions.

Mr. FLORES. I would like to add two things. One is that the Safeguarding Our Children, United Mothers and Cyber Angels has a list, and their estimation is there are approximately 40,000 sites devoted to this type of topic. Whether they range from actual child pornography or pseudo-child pornography, I don't know.

Mr. EHRLICH. When you are talking about 40,000 sites, you are talking about child pornography?

Mr. FLORES. Sites which pander to what would most people would think would be sex, interest of sex with children. But I think that, you know, one of the things that you would normally see is that in most of the Justice Department's prosecutions of child pornography, they really focus on a very—and when I was there, I did the same thing—we focus, we try to say from the bright line, from the age of 18, because quite frankly there are a ton of cases out there and it is like shooting fish in a barrel.

But what it means is that because many of the men and women or boys and girls that are depicted in this pseudo-child pornography can be anywhere between 13 and 18, and they have adult bodies, but these are bodies which also correspond to, you know, a body type of someone without big hips or big breasts or what you would normally acknowledge to be an adult woman. We don't know, because we don't know who those children are. We don't know how old they are. We don't know the pornographer. Is the guy honest in telling us, yes, I have verified, I have checked the birth certificate, I have checked the driver's license? And this is a particularly vulnerable age, especially today.

I remember as a teenager I wanted to be 21 in just a horrible way, and so to be treated as an adult, to be treated as mature, is of great interest. And so we have all of these children that are out there, and I for one as I look at some of these images that are offered as adult, barely legal, just over 18, I wonder if many of them are 13 or 14 and 15. And it would seem to me, even if you didn't want to tackle some areas of adult obscenity, this would be an area that cries out for attention because these are our kids.

Mr. EHRLICH. Well put, and my time is up. Thank you all very much.

Mr. TAUZIN. The Chair recognizes the gentleman from Mississippi, Mr. Pickering, for a round of questions.

Mr. PICKERING. Thank you, Mr. Chairman. I want to thank you for having this hearing today and allowing us a chance to listen to

the panel and to see if there is something that can be done to gather and garner the attention of the public and the Justice Department of the great need to protect our children, to fully enforce both obscenity and child pornography laws. I want to thank Mr. Largent for all of his hard work in this area and being the force behind this hearing.

I think Mr. Largent is right: If we enforced our obscenity laws, a lot of the other efforts that many of us are doing—I have a bill, for example, that would require all schools and libraries to have a filter or a blocking device if they accept an e-rate. In many ways, that could protect our children from many of the harmful effects of both obscenity and pornography as well as other sites that induce violence or hatred that we are seeing in school-age children that have access.

Let me ask Ms. LaRue and other members of the panel, if the Justice Department continues its laissez-faire approach to obscenity, would a national policy for our schools and libraries of finding some protective filter or blocking or some policy, do you think that would be a helpful step as well to protect our children? Ms. LaRue.

Ms. LARUE. Mr. Pickering, this problem is so serious and so pervasive that we have to do everything we can to protect the children of this country and to prevent more victims who will become addicts to this material and to do, as the Supreme Court said, to hope to maintain a decent society.

However, with all due respect, and I certainly support your bill wholeheartedly, and I think you will agree with me, when we talk about filtering and all that parents can do, we are talking about almost Band-Aid applications to an epidemic. To me it is like telling the citizens of a particular community where the dam is breaking. Well, you can go down to the local fire department and get some free sandbags. It is time to fix the dam. It is time to hold those accountable who have jurisdiction over this dam that has burst on this society, to enforce the law and to prevent us from having more victims and turning our libraries into virtual dirty bookstores.

There is an incident in this book, one of the more than 2,000, where a 13-year-old boy in Phoenix, Arizona went into the men's room of the public library and offered a 4-year old boy 25 cents if he could perform a sex act on him. I have a copy of the police report. When the police interrogated this 13-year-old boy about why he did this, where he learned this, he said, I come in here every day and I look at pornography. And, by the way, he just happened to get into a chat room with a pedophile, who dared him to do that very thing, to try to commit a sex act on a younger child.

And so, yes, while I support your bill and I applaud you for it and for others like it, we just can't rely on that. We have to have the Department of Justice enforcing our Federal obscenity laws.

Mr. LAASER. I am sorry to keep interrupting.

Mr. PICKERING. Let me ask you, Mr. Laaser, what are you seeing in your practice as far as children who may be exposed? You had mentioned one case, access of an 11-year-old boy who acted out on what he was seeing at a public library. Are you seeing other children, whether through their school or through libraries, that are

having the manifestations of problems that can really be destructive?

Mr. LAASER. Very definitely. As I think I have said before, we are seeing a rise in the cases of teenagers who are at that age, 12, 13, 14, 15, addicted already to sexuality in general. We are seeing an increase in the numbers of kids. It used to be that you would not expect a 7-, 8-, 9-year-old to present with problems of having seen pornography. Today we are seeing those cases.

Mr. PICKERING. Now, do many of them talk about their access being schools or libraries?

Mr. LAASER. Yes, absolutely. Yes. I mean, you know, parents of minors, parents who are providing Internet filtering devices like the one presented here today, I mean they can still go to their public schools and get it there. I would challenge—and I get myself in trouble. We could go to any public school within a 50-mile radius that has online access and we don't need very many computer skills and we could get into the hardest and most violent core types of pornography.

Mr. PICKERING. Mr. Flores, let me ask, you are legal counsel on the subject of filters for schools and libraries. Yesterday I was very disappointed. When I was working on Senator Lott's staff and on the Telecommunications Act of 1996, I worked on the amendment that would require the cable systems to fully scramble the pornographic or adult sites. That was struck down on a 5-to-4 decision yesterday. It was the Lott-Feinstein amendment.

Would you see any, based on current court precedent decisions, would you see any legal or constitutional challenges to a bill that would require schools and libraries to use filters if they accept the e-rate?

Mr. FLORES. The Supreme Court has provided broad latitude to the Congress to condition receipt of its money on action by State and localities. Obviously it has to be done within certain limits. It is not carte blanche, and I don't think that many Members of Congress really want to impose a straitjacket on any community, but certainly I don't think that there would be a constitutional problem with that. I think that falls probably more into the area of just plain politics.

I would, if I could, just follow up on Dr. Laaser's comments. One of the things that you will hear probably from the Justice Department is about a case called the Orchid Club, and I worked with the assistant U.S. attorneys who were prosecuting that case, and it is such a revolting case that it is hard to really conceive that actions like that took place. But I think that is part of the issue, is that there is a sense of lawlessness on the Internet because the marshal is not there. I mean, there just does not seem to be—and this cuts across a number of areas from copyright and fraud, penny stock manipulation.

The other issue is that the Justice Department is spending a substantial amount of money working on important efforts, things like violence against women, trying to make sure that there aren't unconstitutional glass ceilings, making sure that girls get access to science and math programs. And all of these are jeopardized if we have a generation of boys who are going to grow up addicted to material which teaches them that girls like sex with humiliation and

pain; that the secretaries really—that is her job, is to make the boss happy, not to really carry out official business. I mean, this sends just horrible messages which undermine—even the date rape drug, Rohypnol, that Attorney General Reno focused on a number of years ago, we are going to see an explosion in date rape because this material teaches one consistent message: No does not mean no. And the early Playboy philosophy was that it is every man's job in life to relieve women of that nasty little fact, their virginity. This is a consistent message and it places even DOJ programs at jeopardy.

Mr. TAUZIN. The gentleman's time has expired. We are faced with a choice here that I want to perhaps ask your assistance, Mr. Gershel. We are finished with this panel, and what I would like to do is give everybody a lunch break and come back at 1:30 if that's acceptable to you.

Mr. GERSHEL. That will be fine.

Mr. TAUZIN. While he is discussing it, let me take care of a point of business and get back to you. Ms. LaRue, we have examined with legal counsel your request. If you would like to reenter your request we can accept your material provided that it be filed in the permanent record of this proceeding, not for duplication, which is the normal process I think. Is that acceptable?

Ms. LARUE. It certainly is.

Mr. TAUZIN. Then, without objection, her material will be accepted by the committee, filed in our permanent record.

The gentleman from Texas.

Mr. GREEN. Mr. Chairman, I understand there is a committee hearing in this room, at 2:30 in this room. Even more so, I would like to follow up while we are discussing, and I understand Ms. Stewart with FamilyClick.com actually has an Internet service that libraries could buy that is between the ISP and the libraries, and I would just like to know that because I think—in fact, I agree with my colleague from Mississippi's legislation, and I know the technology is there to be able to do that.

Mr. TAUZIN. Let me recognize the gentleman to ask that question while I discuss with Mr. Largent.

Mr. GREEN. Is that correct? And I apologize for not being here earlier because of votes and everything else. Is that true that the Houston public libraries and my Harris County public library in Houston can actually purchase that ability right now to have that?

Ms. STEWART. Yes, sir. There are many filtering companies that provide filters, some better than others. The filters do a great job of protecting innocent searching, blocking, you know, the things that I pointed out. But if you want to find pornography, or you go in there for a specific purpose, you will find it. There is no way for us to block it all because it is coming online so fast every day. And also the images, we do not have the technology available right now to scan the images. We are testing with it. It runs on great multimillion dollar computers and it is impossible for us to put that online right now.

Mr. TAUZIN. The Chair will put Mr. Largent in the chair and we will continue the hearing so that we don't have to—unfortunately, we won't have a lunch break, but that I think will keep everybody in the room.

So, Mr. Gershel, we will proceed on time. Let me thank this panel very much and we appreciate your attendance. The record will stay open for 30 days. If you have additional information or submittals, you are perfectly free to do so, and members may have written questions within the 30-day period of time they want to send you.

Again, thank you for your testimony and let me particularly thank you the two of you for your personal observations on your own personal history with this issue.

We will now call the second panel, Mr. Alan Gershel, the Deputy Assistant Attorney General, Criminal Division, Department of Justice. Mr. Gershel, I was unhappy about the discussion we had this morning. I am very happy you stayed and listened to this panel, and what you have heard today may be a backdrop in terms of what you want to tell us in terms of the Justice Department's position on enforcing these criminal statutes. I thank you for being courteous enough to sit through the first panel and to hear their testimony.

The Chair will ask you again, as we ask all our panelists to, without objection, that the written statement of Mr. Gershel is a part of the record, without objection. Mr. Gershel, we will be generous in terms of providing you additional time to make your presentation, and the Chair now recognizes you for that and recognizes Mr. Largent in the Chair.

Mr. LARGENT [presiding]. Go ahead, Mr. Gershel.

STATEMENTS OF ALAN GERSHEL, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE; ACCOMPANIED BY TERRY R. LORD, CHIEF, CHILD EXPLOITATION AND OBSCENITY SECTION, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Mr. GERSHEL. Mr. Chairman, good morning. Sitting on my right, I would like to introduce Mr. Terry Lord. He is the chief of the Child Exploitation and Obscenity Section. He is joining me up here this morning as well.

Mr. Chairman, I welcome this opportunity to speak about the achievements of the Department of Justice regarding its prosecution of illegal use of the Internet to exploit our children. In the brief time that I have today, I would like to highlight what the Department of Justice has been doing. At the outset, I have heard the testimony about the proliferation of obscenity on the Internet. I know there are victims of Internet obscenity and that obscenity has damaged the fabric of many marriages.

The Federal Government takes seriously its mandate to prosecute obscenity cases, and each year various United States Attorneys bring obscenity prosecutions against material they deem is obscene according to their own community standards.

In considering the question of how to address illegal material that proliferates on the Internet, however, the Attorney General has given the investigation and prosecution of cases involving the use of minors in producing pornography the highest priority, and I can assure you that the Department will continue to do so.

The visual representations of children engaged in sexual activity are the most pernicious form of obscenity because it necessarily in-

volves an unconsenting victim. I would like to tell you about some of our efforts in this area.

Child pornography prosecutions are at a nationwide all time high. According to figures provided to us by the executive office of the United States Attorneys, in fiscal year 1999, United States Attorneys filed 510 Federal child pornography cases concerning 525 defendants. During that same period, 378 persons were convicted. In fiscal year 1999, the Department had a 90 percent conviction rate. This increase reflects in part our national effort to prosecute those who utilize the Internet to exploit our children.

Here in Washington, D.C., the Criminal Division continues to coordinate the Department's efforts to prosecute traffickers of child pornography. Most recently, the United States Attorney's Office for the Northern District of Texas indicted five individuals.

Mr. LARGENT. Mr. Gershel, if you will excuse me just for a second, we understand the Department has an excellent record on prosecution of child pornography. However, that is not what this hearing is about. So if you want to go ahead and cite statistics about things that this hearing has nothing to do with, that is fine, I will let you continue. But again, the focus of this hearing is on the prosecution of obscenity, not child pornography. You may continue.

Mr. GERSHEL. Thank you, Mr. Chairman. With all due respect, we take the view that child pornography is the worst kind of obscenity, and we believe that it is a primary mission of the Child Exploitation Section at this time. I would like to continue with my statement. It is much along the same lines.

As I indicated, here in Washington, the Criminal Division continues to coordinate the Department's efforts to prosecute traffickers of child pornography. In the case I just mentioned it involved five individuals, two Americans, one Russian, and two Indonesians, in a multiple-count indictment with sexual exploitation of minors, distribution of child pornography, aiding and abetting and criminal forfeiture. The two American defendants operated a credit card verification service that acted as an electronic gateway to the pictures and movies of minors' sexually explicit conduct. Also as part of the conspiracy, the American defendants operated a bulletin board service to capture customers, notices, promotions, advertisements and images of child pornography in order to market, advertise, and promote child pornography by computer.

The Child Exploitation and Obscenity Section in collaboration with the FBI also helped to coordinate the Innocent Images project which was organized in 1995 to combat the trafficking of child pornography over computer networks. CEOS, as it is called, continues to work closely with the FBI on the Innocent Images project. The FBI is currently creating regional task forces to work these cases, and CEOS participates in training with the task force personnel.

The CEOS works closely with United States Customs Service and its Cyber Smuggling Center, which has several undercover operations in effect. CEOS is working with the Customs Service on Operation Cheshire Cat, an international child pornography investigation. This operation was an outgrowth of the Orchid Club case to which I have referred in my written testimony.

For the preparation for this project, CEOS worked with the Customs Service in 28 Federal districts to develop search warrant affidavits and provide other guidance. CEOS continues to provide technical assistance on this and other Customs Service child pornography projects.

The Department also works closely with the United States Postal Inspection Service which has developed numerous undercover operations targeting Internet child pornographers who use the U.S. mail to ship child pornography materials. CEOS is currently working with the Postal Service on projects looking at the Web postings offering child pornography to be shipped via the mail.

Our efforts to protect children using the Internet have not stopped at the national level, however. The Office of Juvenile Justice and Delinquency Prevention, OJJDP as it is called, in fiscal years 1999 and 2000 has provided funding for the establishment of 30 Internet Crimes Against Children Task Forces in several regions around the country that involve local, State, and Federal law enforcement working together on these crimes against children.

Two attorneys from CEOS have been assigned as legal advisers to the task forces, and they regularly participate in the training programs for the task force personnel.

We are also working with new tools enacted by Congress that enable us to quickly acquire information about violators from Internet service providers and to subpoena identifying information. Pursuant to the Protection of Children from Sexual Predators Act of 1998, Internet service providers are required to report incidents of child pornography on their system through the appropriate Federal agency. In November 1999, Congress amended the statute to require providers to report such incidents to the cyber tip line operated by the National Center for Missing and Exploited Children, which in turn contacts Federal and State law enforcement.

The Protection of Children from the Sexual Predators Act also granted administrative subpoena authority to the Department in cases involving child abuse and child sexual exploitation. The Attorney General has delegated the FBI, criminal division of the Department, and the United States Attorneys' offices with power to issue these administrative subpoenas to Internet service providers who require specified identifying information about those who unlawfully use the Internet to sexually exploit children.

The Department has also facilitated prosecution of Internet crimes against children on the international front as well. In September and October 1999, the Department attended an international conference on combating child pornography on the Internet in Vienna, Austria. We played a major role in the planning of this conference. During this conference, an Internet service provider discussed the development of an industry code of conduct to combat child pornography online and made several recommendations for the type of issues that must be covered.

CEOS also works internationally with the European Union and the Council of Europe to develop protocols to combat child pornography. These protocols, which are still being negotiated, cover not only substantive criminal law regarding what conduct all countries must prescribe but also procedural guidelines for investigations that necessarily are international in scope.

What I have presented today highlights just some of our efforts the Department of Justice has made to protect our families online. We have made a strong commitment to our child protection efforts and this commitment will continue.

Thank you again for the opportunity to appear before the committee today. I will be happy to try and answer any questions, Mr. Chairman.

[The prepared statement of Alan Gershel follows:]

PREPARED STATEMENT OF ALAN GERSHEL, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Mr. Chairman and Members of the Subcommittee: I appear today to discuss a matter of importance to us: the proliferation of pornography on the Internet and the danger to children that can result from the use of the Internet for unlawful activity.

1. In considering the question of how to address illegal material that proliferates on the Internet, the Attorney General has given the investigation and prosecution of cases involving the use of minors in producing pornography the highest priority, and I can assure you that the Department will continue to do so. Visual representations of children engaged in sexual activity are the most pernicious form of obscenity because it necessarily involves an unconsenting victim. As an example, the Department recently prosecuted a child pornography production ring, known as the "Orchid Club." Members of the "club" requested and received real time images of children being molested in front of video cameras that relayed the pictures to members via the Internet.

Furthermore, with the prevalence of computers and easy Internet access, there has been a rapid increase in crimes involving trafficking in child pornography and use of the Internet to meet children for sexual activity.

The Department has devoted a large portion of its resources to prosecute aggressively this increased threat to children. Over the past four years, the Child Exploitation and Obscenity Section's (CEOS's) original mandate to prosecute obscenity, including child pornography, has been greatly expanded. The Section is now also tasked to prosecute additional crimes that have child victims. Since Fiscal Year 1996, the information we provided to Congress to support our budget request included a description of the expanded mission.

The most recent budget submission to Congress (for FY 2001 now pending) described CEOS as a section that prosecutes and assists United States Attorneys in prosecuting persons who, under the federal criminal statutes: possess, manufacture, or distribute child pornography; sell, buy or transport women and children interstate or internationally to engage in sexually explicit conduct; travel interstate or internationally to sexually abuse children; abuse children on federal and Indian lands; do not pay certain court-ordered child support payments; transport obscene material, including child pornography, in interstate or foreign commerce either via the mails, common carrier, cable television lines, telephone lines or satellite transmission; and engage in international parental child abduction.

CEOS attorneys assist United States Attorneys Offices (USAOs) in investigations, trials, and appeals related to these statutes. Additionally, CEOS attorneys provide advice on victim-witness issues, and develop and refine proposals for prosecution policies, legislation, governmental practices and agency regulations in the areas of sexual exploitation of minors, child support and obscenity for USAOs, United States Customs Service, United States Postal Service, and the FBI. CEOS also conducts and participates in training of federal, state, local and international prosecutors, investigators and judges in the areas of child exploitation and trafficking of women and children.

The Child Exploitation and Obscenity Section has coordinated several investigation and prosecution programs to combat the use of computers and computer bulletin board systems that traffic in child pornography. These programs specifically target the illegal importation, distribution, sale and possession of child pornography by computer, as well as individuals who attempt to solicit children online for exploitation. These investigations often utilize undercover agents, posing as children, but who are trained not to engage in activities that might constitute entrapment.

Our efforts have produced striking results. In the past five years, we have seen an increase in child pornography cases filed from 127 in fiscal year 1995, to 510 cases filed in fiscal year 1999. We have seen similar increases in cases filed under statutes prohibiting using the Internet to entice a child for illegal sexual activity,

and traveling in interstate commerce for the purposes of meeting a child for illegal sexual activity.

2. We have also worked closely with the Civil Division in defending the Child Online Protection Act (COPA), as enacted by Congress in 1998. As recently recognized by the district court reviewing the Child Online Protection Act, it is undisputed that "sexually explicit material exists on the Internet," including the World Wide Web. This material includes "text, pictures, audio and video images," and "extends from the modestly titillating to the hardest core." The House Report on COPA estimated that there were approximately 28,000 Web sites promoting pornography, and that these sites generated "close to $925 million in annual revenue." H.R. Rep. No. 105-775, at 7 (1998).

Congress first sought to address the problem of children's access to sexually explicit materials on the Internet in section 502 of the Communications Decency Act ("CDA"), enacted in 1996. The CDA prohibited the knowing transmission of obscene or "indecent" messages over the Internet to persons under the age of 18, 47 U.S.C. § 223(c) (Supp. II 1996), as well as the sending or display of patently offensive sexually explicit messages in a manner available to those under 18 years of age. 47 U.S.C. § 223(d). The statute provided, however, that it would be an affirmative defense to prosecution for those persons who had "taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors" to those communications covered by the statute, or who had restricted access to a covered communication "by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number." 47 U.S.C. § 223(e)(5) (Supp. II 1996).

On June 26, 1997, the Supreme Court held the CDA unconstitutional under the First Amendment. *Reno v. ACLU,* 521 U.S. 844 (1997). The Court noted that it had previously agreed that the government has a "'compelling interest in protecting the physical and psychological well-being of minors' which extend[s] to shielding them from indecent messages that are not obscene by adult standards." 521 U.S. at 869 (citation omitted). But, emphasizing that the "breadth of the CDA's coverage" was "not limited to commercial speech or commercial entities," and that "[t]he general, undefined terms 'indecent' and 'patently offensive'" would "cover large amounts of non-pornographic material with serious educational or other value," *id.* at 877, the Court invalidated the statute because it "place[d] an unacceptably heavy burden on protected speech." *Id.* at 882.

With the invalidation of the CDA, Congress renewed its efforts to address the problem of children's access to sexually explicit material on the Internet. As the House Commerce Committee observed, while the Internet is "not yet as 'invasive' as broadcasting, its popularity and growth because of electronic commerce and expansive Federal subsidy programs make it widely accessible for minors." House Report, at 9. "Moreover," the Committee explained, "because of sophisticated, yet easy to use navigating software, minors who can read and type are [as] capable of conducting Web searches as easily as operating a television remote." Id. at 9-10. The Committee found that purveyors of sexually explicit material "generally display many unrestricted and sexually explicit images to advertise and entice the consumer into engaging into a commercial transaction," id. at 10, and that the availability of such material to minors demonstrated a continued need for legislation to protect children from the effects of unrestricted exposure to such material. The Committee emphasized the government's compelling interest in protecting children from exposure to sexually explicit material and noted that legislatures have long "sought to shield children from exposure to material that could distort their views of sexuality," whether by "requir[ing] pornography to be sold behind the counter at a drug store, on blinder racks at a convenience store, in a shrink wrap at a news stand, or broadcast between certain hours of the night." *Id.* at 11.

In the end, after examining the matter in hearings by committees in both Houses, Congress found that the "widespread availability of the Internet" continues to "present[] opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control." Pub. L. No. 105-277, § 1402(1), 112 Stat. 2681-736 (1998). Moreover, it stated, "while the industry has developed innovative ways to help parents and educators restrict material that is harmful to minors though parental control protections and self-regulation, such efforts have not provided a national solution to the problem of minors accessing harmful material on the World Wide Web." *Id.* § 1402(3). As a result, Congress passed and the President signed into law the Child Online Protection Act ("COPA"), Pub. L. No. 105-277, §§ 1401-1406, 112 Stat. 2681-736 to 2681-741 (1998) (to be codified at 47 U.S.C. § 231).

COPA authorized the imposition of criminal and civil penalties on any person who "knowingly and with knowledge of the character of the material, in interstate or for-

eign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." 47 U.S.C. § 231(a)(1). Under COPA, "[a] person shall be considered to make a communication for commercial purposes only if such person is engaged in the business of making such communications," 47 U.S.C. § 231(e)(2)(A). In addition, "material that is harmful to minors" includes only "matter . . . that is obscene as to minors." 47 U.S.C. § 231(e)(6).

Congress established an "affirmative defense to prosecution" if a defendant "in good faith, has restricted access by minors" to the material covered by the statute, by requiring, among other things, the "use of a credit card, debit account, adult access code, or adult personal identification number" in order to access covered material. 47 U.S.C. § 231(c)(1)(A).

In passing COPA, Congress meant to "address the specific concerns raised by the Supreme Court" in invalidating the CDA. *House Report,* at 12. Thus, COPA applied, not to all Internet communications, but "only to material posted on the World Wide Web." *Ibid.; see* 47 U.S.C. § 231(a)(1). As a result, COPA "does not apply to content distributed through other aspects of the Internet," including e-mail, listservs, USENET newsgroups, Internet relay chat, or real time remote utilization, such as telnet, or non-Web forms of remote information retrieval, such as file transfer protocol (ftp) or gopher, all of which would have been affected by the CDA. *House Report,* at 12.

The character of the material covered by COPA was significantly different than that covered by the CDA. The CDA applied to Internet communications that contained "indecent" or "patently offensive" sexual material. 47 U.S.C. §§ 223(a)(1)(B), 223(d) (Supp. II 1996). By contrast, COPA applied to material that is "harmful to minors," 47 U.S.C. § 231(a)(1), that is, material that not only contains a patently offensive depiction or description of sexual activities or sexual contact, but that the average person, applying community standards, would find is designed to appeal to or pander to the "prurient interest," and, as important, lacks "serious literary, artistic, political, or scientific value for minors." 47 U.S.C. § 231(e)(6). *See House Report,* at 13.

Congress emphasized that, in using the "harmful to minors" formulation, it was employing a standard that "has been tested and refined for thirty years to limit its reach to materials that are clearly pornographic and inappropriate for minor children of the age groups to which it is directed." *House Report,* at 28.

In addition, COPA applied only to those Web communications that are made "for commercial purposes," 47 U.S.C. § 231(a)(1), *i.e.,* only if the person is "engaged in the business" of making such communications. 47 U.S.C. § 231(e)(2).

Congress adopted COPA only after considering and rejecting alternative means of protecting children from harmful material on the Web, emphasizing that such alternatives "generally involve[d] zoning and blocking techniques that rely on screening material after it has been posted on the Internet or received by the end-user." *House Report,* at 16. In Congress's opinion, it was "more effective to screen the material prior to it being sent or posted to minors." *Ibid.*

The President signed COPA into law on October 21, 1998. The following day, the American Civil Liberties Union, joined by a number of individuals and organizations that publish content on the World Wide Web, filed a suit in federal district court in Philadelphia, contending that the statute violated their First and Fifth Amendment rights.

The Department vigorously defended the constitutionality of the statute. Nonetheless, on November 20, 1998 nine days before the statute would have gone into effect, the district court entered a temporary restraining order ("TRO") enjoining COPA's enforcement. After a five day evidentiary hearing in January, 1999, the court entered a preliminary injunction on February 1, 1999. **Neither ruling affected materials that are "obscene" or that are child pornography.**

The Department appealed the decision to the Third Circuit, making much the same arguments as in the district court. The case was argued in November 1999. We are waiting for the Third Circuit to rule on the cases.

In the meantime, we are prohibited from prosecuting "harmful to minors" material, although we are free to prosecute material on the Internet that is obscene and that is child pornography.

3. As I have stated, the Department is vigorously enforcing our child pornography laws as they apply to the Internet. We are also enforcing our obscenity laws, as they apply to the Internet. We do investigate and prosecute transmission of obscenity over the Internet, where appropriate. Last fall, the Assistant Attorney General for the Criminal Division met with members of public interest groups who were concerned about the prevalence of Internet obscenity, particularly on World Wide Web sites. At the meeting, the groups submitted a list of hundreds of Web sites that,

in their view, were possibly illegal. The Department agreed to review these sites for possible referral to an investigative agency.

After a thorough consideration of each referral, the Department concluded that the vast majority could not be referred. In our view, many sites failed to meet the three prong test for obscenity as delineated in the *Miller v. California* case. Nonetheless, several sites were deemed appropriate for further investigation and were referred to an investigative agency.

In conclusion, we all agree that we must continue to work to protect our children and the public at large from those who use the Internet to exploit children and to distribute illegal obscenity. We look forward to working with you in achieving that goal.

Mr. LARGENT. Thank you, Mr. Gershel, and I would tell you that if in fact this committee holds a hearing on child pornography, that will be important testimony that you have just submitted and we will reflect on that. However this hearing is about obscenity and the lack of prosecutions thereof.

How long have you been at the Department of Justice Mr. Gershel?

Mr. GERSHEL. Mr. Chairman, my background is I began with the U.S. Attorney's Office in Detroit in 1980. I served there for almost 20 years. I am currently there as both the criminal chief and the first Assistant U.S. Attorney and I am down here in Washington on a detail beginning in January for 1 year as a Deputy Assistant Attorney General.

Mr. LARGENT. And how many obscenity cases has the Department prosecuted since 1996? Not child pornography; obscenity.

Mr. GERSHEL. I believe we have furnished statistics which would indicate approximately 14, 15, perhaps as many as 20 obscenity cases.

Mr. LARGENT. Those are obscenity cases exclusive of child pornography?

Mr. GERSHEL. Exclusive of child pornography.

Mr. LARGENT. In other words, child pornography had nothing to do with the cases that were brought? It was strictly obscenity cases in the last 4 years, 14?

Mr. GERSHEL. Excuse me 1 second.

Mr. LARGENT. The reason I ask the question, of course, Mr. Flores testified that sometimes they are tacked together.

Mr. GERSHEL. Mr. Chairman, if I might, Mr. Lord might be able to specifically answer that question dealing with statistics.

Mr. LORD. Mr. Chairman, in all of those cases, obscenity counts were charged and there were convictions. There may have been other charges brought in those indictments, but obscenity counts were charged and those are the statistics. There is no question about obscenity cases being brought.

Mr. LARGENT. Okay. So we have testimony that between 1989 and 1995 the Justice Department's Child Exploitation and Obscenity Section, which you are a part of today, actually not brought but had 126 individual and corporate convictions with obscenity violations, not child pornography; 126 individual and corporate convictions for obscenity violations which resulted in the imposition or award of more than $24 million in fines and forfeitures.

My question is: Since 1996, how many convictions have there been of individuals or corporate entities for obscenity violations—obscenity violations—and how many dollars in fines and forfeitures have occurred?

Mr. GERSHEL. Mr. Chairman, we don't have those figures available. We can furnish them to the committee at a later time and would be happy to do so.

Mr. LARGENT. I would take an estimate.

Mr. GERSHEL. We just don't have the information. Of forfeiture, we don't have the information.

Mr. LARGENT. But you are responsible for the Child Exploitation and Obscenity Section?

Mr. GERSHEL. I oversee that section.

Mr. LARGENT. Is it Terry?

Mr. GERSHEL. Yes, sir.

Mr. LARGENT. You are the head of the Child Exploitation and Obscenities Section?

Mr. LORD. Yes, I am.

Mr. LARGENT. And you don't have any idea?

Mr. LORD. I can get you the exact amount of forfeiture involved in those cases, Mr. Chairman. I wasn't asked to provide those today.

Mr. LARGENT. That was the purpose of the hearing. I think you got notice of that.

Let me go on. What is the problem? Is this a personnel and money issue? Do you not have the personnel, don't have the money available to prosecute obscenity?

Mr. GERSHEL. Mr. Chairman, no, I think the answer is that the current priorities are in fact child pornography, which is the worst, most vile form of obscenity.

Mr. LARGENT. We all agree with that.

Mr. GERSHEL. That is where the resources of the Justice Department, both here in Washington and in the 94 U.S. Attorneys Offices, are being primarily devoted, to the prosecution, investigation and conviction of those who victimize our children.

Mr. LARGENT. Exactly. So what happened to the $1 million that the Congress appropriated to the Department of Justice to prosecute not child pornography but obscenity, what has happened to that money? How have you spent that money?

Mr. GERSHEL. Mr. Chairman, I don't want to quibble with you but that money was earmarked, as I understand, for the prosecution of obscenity cases. We continue to take the view that child pornography is in fact obscenity, and that money was utilized to hire more prosecutors to engage in those efforts.

We have instituted a number of sophisticated training programs for prosecuting agencies around the country. We have used that money to help buy equipment, laptop computers for people engaged in that effort. That money was spent, well spent, and devoted to the prosecution of the worst kind of obscenity.

Mr. LARGENT. Well, frankly, I am astounded that the gentleman that is responsible for this investigation is confusing or merging two terms, legal terms of art, that everybody understands are mutually exclusive. Obscenity is not the same as child pornography. And so when Congress says we appropriate $1 million to prosecute obscenity, we are not talking about child pornography. We gave you money for that, too. We are talking about obscenity. What happened to the $1 million to prosecute obscenity, not child pornography?

Mr. GERSHEL. I believe I have answered your question, sir.

Mr. LARGENT. I don't think you have answered my question. Maybe you can submit that in writing at another time as well.

Mr. PICKERING. Mr. Chairman, I am afraid he did answer your question, if you would yield just a second. They didn't do it, they don't know anything about it.

Mr. LARGENT. I think I have just a little bit of time left before I yield. Mr. Gershel, do you have any idea who the largest producers and distributors of hard-core, sexually explicit material are?

Mr. GERSHEL. As we sit here now, I could not give you that information, no.

Mr. LARGENT. Does the Department know?

Mr. GERSHEL. I believe that they have intelligent information on some of those issues, yes.

Mr. LARGENT. But you are not sure?

Mr. GERSHEL. I believe they do.

Mr. LARGENT. Can you produce those?

Mr. GERSHEL. That would depend, sir. If those matters are under investigation I would be reluctant to produce that information at this point in time.

Mr. LARGENT. I would like to yield to the gentleman from Ohio, Mr. Sawyer.

Mr. SAWYER. Thank you, Mr. Chairman. I guess I have some substantial sympathy with the notion that there is no worse form of obscenity than the exploitation of children for sexual purposes and that I would take the view, Mr. Chairman, that the question was asked several times and that in fact that $1 million was devoted to the pursuit of the worst form of obscenity that the Justice Department deals with. It seems to me we sat here for——

Mr. PICKERING. Would the gentleman yield just for a second?

Mr. SAWYER. I am not going to yield. The Chairman went on at some length, and we sat here this morning and we listened for extended periods of time to testimony about just how dangerous pedophilia is, how threatening it is in the lives of ordinary people who wind up being victimized by this sort of thing. And to argue that that somehow this is not obscenity I think is to beg the question.

Having said that, this morning there was a good deal of testimony about the failure of the Justice Department to undertake the kind of work that at least the panelists who were with us this morning felt ought to have been undertaken. Would you care to comment on that testimony that preceded you this morning?

Mr. GERSHEL. Congressman, a couple of comments. First of all, the——

Mr. SAWYER. Could you bring the microphone closer? Those are very directional mikes. You have really got to get it——

Mr. GERSHEL. First of all, I listened to most of the testimony, both the statements and the questions, and it was clear to me and I am sure to my colleagues that these are very strongly held beliefs. I certainly cannot begin to understand the trauma that the gentleman went through who was addicted to pornography, and I am not going to try in any way to argue with that. But what I would like to say, though, is that we have established prosecutor guidelines for prosecution of obscenity cases, that is, cases not deal-

ing with child pornography, and we believe those guidelines are appropriate under the circumstances. They deal with the investigation of what we believe to be major national and international pornographers. It has been our belief and experience that oftentimes these groups, as has been mentioned, are funded by organized crime activities. We believe that these investigations are time consuming, they are complex. They often involve charges in addition to obscenity. They may involve RICO charges, money laundering offenses and things of that nature.

I should also indicate, if I can have one more moment to respond to your question——

Mr. SAWYER. Sure.

Mr. GERSHEL. [continuing] that one of the comments made by Mr. Flores I do happen to agree with. There were more than one, but this one in particular. When discussing child pornography, I believe he used the expression "tons of cases" and "shooting fish in a barrel," and unfortunately that probably is true.

Shortly after I came to Washington I asked for a tour of the Innocent Images project, and while touring the project we actually had an online demonstration, and an FBI agent went on line into chat rooms that had been determined to consist of people engaging in this kind of activity; that is, child pornography. He posed as a 14-year-old girl. And sir, within 5 minutes, with no effort on his part, he was able to engage in a conversation with this person. Now, mind you, this is the middle of the work day, and with a little more effort, I am sure he could have arranged a meeting with this individual, and that was pure happenstance, pure chance, just part of the tour of the Innocent Images. They had their hands full, unfortunately, with just keeping up with the work that is out there, and that is again where the resources of the Department are going to be devoted, to the prosecution of child pornography.

Mr. SAWYER. Thank you, Mr. Chairman. I yield back. I yield to my friend from Mississippi.

Mr. PICKERING. Yes, and let me just, you know, again for the record, not of policy, not of emotion, but as I understand it, the law, that there is a difference in the law between child pornography and obscenity. And I can read the obscenity statute or the definition of obscenity and I can read the definition of child pornography. You know, the Justice Department, I think, is fully aware of this. I don't want to——

Mr. SAWYER. I appreciate the gentleman's comment and I do understand that. Reclaiming my time, would the witness care to respond to the assertion?

Mr. GERSHEL. Excuse me one moment. Congressman, we do agree they are not the same, but it is our view that they do substantially overlap. So if I said it was exactly the same, that was a misstatement. I stand corrected. We do believe there is a substantial overlap.

Mr. SAWYER. Mr. Chairman, I would like to withdraw from this conversation, and perhaps the gentleman from Mississippi could——

Mr. LARGENT. The gentleman's time has expired. The Chair recognizes the gentleman from Mississippi for 5 minutes.

Mr. PICKERING. And I think you just made my point for me. There is significant overlap. There is significant interaction. There is significant contribution, one to the other. A culture of obscenity leads to a greater culture and exploitation of children, and the Justice Department, although I would agree with them in making a targeted effort on child pornography, and most everyone in the country and on this committee would agree that child pornography is the worst manifestation, but where this committee is trying to go and trying to reach common ground with the Justice Department is that you cannot just address one.

You have probably seen at the Justice Department, I would think you would agree, a rise in the exploitation of children and child pornography over the last 3 to 4 years. Would that be an accurate statement?

Mr. GERSHEL. Dramatic increase.

Mr. PICKERING. A dramatic increase. One of the reasons I believe you have the dramatic increase is because of the lax enforcement or the lax effort to address obscenity. They overlap, they are integrated, they contribute to each other. And until you address both, you are going to continue to see a dramatic increase.

So maybe let us see if we can find common ground. If we, for example, we gave $1 million just for the enforcement and prosecution of child obscenity, let us say that we gave you $10 million for the enforcement, $50 million—you pick the number, whatever it would take for you to do it—if we did that, would the Justice Department policy change from being a child pornography-only to a child pornography and obscenity enforcement and prosecution policy?

Mr. GERSHEL. Congressman, with all due respect, I take some exception to the question because I don't believe that CEOS is exclusively child pornography; primarily, but not exclusively. Also, I am not in a position to comment about the change in Department policy.

Mr. PICKERING. Could I interrupt just a second? And, again, I want to listen to you. One, you have been asked questions of what is the status of your obscenity prosecutions since 1996 or who are the major producers. You couldn't even tell the committee those two questions, which is an indication that that has not been your priority nor your practice. I yield back.

Mr. GERSHEL. I would stipulate it has not been a priority. I should indicate though that we have not ignored the problem.

There was a reference during the previous panel's testimony to a meeting that was had with the Assistant Attorney General and some other individuals. Although I was not present for that meeting, I understand that during the course of that meeting a number of Web sites, for example, were furnished to the Criminal Division for review.

I should indicate that the CEOS section has undertaken a comprehensive review of those Web sites, taking several months, and in fact a number of those have been referred to the FBI for further investigation and they are currently under investigation.

Mr. PICKERING. Although in your testimony you say, After a thorough consideration of each referral, the Department concluded the vast majority could not be referred. Nonetheless, several sites were deemed appropriate for further investigation and were referred to

an investigative agency." So out of hundreds of examples, you referred how many for further investigation?

Mr. GERSHEL. Mr. Chairman, may I allow Mr. Lord to respond to this question?

Mr. LORD. Congressman, I am not going to comment on the specific number that we referred. I do want to say that we gave proper legal analysis to all of those referrals. That is not normally done. Most of the time in these types of cases, the investigators conduct that type of investigation, but we deemed it important enough for section attorneys to make that review and to give their comments to the FBI. Those comments were given to the FBI in terms of what type of analysis we gave to it. We didn't make any predisposition of how they should review the case. So it's improper to say that we only referred a small number. We actually turned over the same material that was given to us to the FBI, but with our analysis.

I also want to comment——

Mr. PICKERING. Just interrupting real quickly, I just read from your own testimony. You describe it in your own testimony.

Mr. LORD. I am just clarifying that, Congressman. Another point I want to make about this and your trying to separate obscenity from child pornography, the techniques for investigation of child pornography and obscenity, of course, are very similar. It involves online undercover activities; our work with the State and local Internet crimes against children, training them to investigate online dissemination of the materials; our work with the European Union, the Council of Europe. I also serve on Interpol Standing Committee on Offenses Against Children. All involve these types of techniques, working with Internet service providers, attempting to have data retention, zero tolerance for this activity. All relate to obscenity just as well as child pornography.

So the funds that we were given to investigate online obscenity were used to develop those types of techniques with the European Union, with State and local investigators, which will improve our efforts in investigating both obscenity and child pornography.

Mr. LARGENT. The gentleman's time has expired. I recognize the gentleman from Texas.

Mr. GREEN. Thank you, Mr. Chairman. I appreciate the Justice Department being here today, and I apologize in some cases for the adversarial relationship I guess we have, but obviously you know how important it is for all of us. In fact, I have had the opportunity to meet with the FBI in my own district and talk to the FBI investigator about child pornography on the Internet, what they can do to help us. In fact, they have actually presented programs in our public schools, and we are trying to do one for parents later on, what parents can do to keep their children from being subjected to pornography over the Internet.

And so I think it is a multifaceted effort, not just for the prosecution, but also with the FBI doing what they can, and also with Internet service providers, I know; not to say one, but AOL also helped us.

One of my questions, Mr. Gershel, is the Department of Justice, FBI, in your latest efforts on catching pedophiles and using the Internet to track children and child pornography, how is the Fed-

eral Government expanding the enforcement in this area and what, if anything, are you doing with local communities like, for example, the State agency, the Department of Public Safety in Texas as well as our local police agencies?

Mr. GERSHEL. Congressman, we have, I believe, entered into a very strong and solid partnership with our State and local investigative and prosecutive agencies, and many of these task forces that I referred to in my comments. They are devoted to looking for instances of child pornography, but obscenity as well. So we believe we have established a good relationship, and cases are being developed both at the Federal and the local level in these areas.

Mr. GREEN. The second question, let me ask—I know some of the frustration often deals with our different roles we have; and, as a Member of Congress, what I consider may be obscene is not necessarily what the folks across the street at the Supreme Court may agree. I know we heard in an earlier panel Dr. Laaser talked about what he considered—I may share that, but, again, the Justices of the Supreme Court may not—one of the frustrations we have is that in 1998 this committee—or 1997 to 1998 passed the COPA Act, the Child On-line Protection Act, and I know also in your testimony you discussed a Community Decency Act that was struck down by the Supreme Court. And now the COPA Act is being challenged, and the Justice Department is appealing that, and I asked an earlier panel if there was any update on that. Is that still before the appeals court?

Mr. GERSHEL. Still before the Third Circuit.

Mr. GREEN. Did the Department of Justice provide Congress with any suggestions on how to improve the COPA legislation so that we might pass legislation that would be perfected from constitutional challenge?

Mr. GERSHEL. I am sorry, Congressman.

Mr. GREEN. Do you recall, did the Justice Department provide Congress with any suggestions when we were considering the child on-line pornography act on how we can try and pass legislation that would withstand a constitutional challenge.

Mr. GERSHEL. I believe the Justice Department worked closely with the committee to try and draft the statute that would withstand challenges, and I think we were at the table with this committee during that process.

Mr. GREEN. Mr. Chairman, I would like to ask unanimous consent to place in the record a letter sent on October 5, 1998, to our Chair, that is, from the Department of Justice, discussing H.R. 3783, which is the Child On-line Protection Act which I think might be—if the Justice Department's suggestions have been taken, we might have at least dealt with some of the issues that are now before the appeals court.

Mr. LARGENT. Without objection.

[The information referred to follows:]

U.S. Department of Justice
Office of Legislative Affairs

COPA

TO DISF DS AL File

Office of the Assistant Attorney General

Washington, D.C. 20530

October 5, 1998

The Honorable Thomas Bliley
Chairman
Committee on Commerce
U.S. House of Representatives
Washington, DC 20515

This letter sets forth the views of the Department of Justice on H.R. 3783, the "Child Online Protection Act" ("the COPA"), as ordered reported. We share the Committee's goal of empowering parents and teachers to protect minors from harmful material that is distributed commercially over the World Wide Web. However, we would like to bring to your attention certain serious concerns we have about the bill.

The principal provision of the COPA would establish a new federal crime under section 231 of Title 47 of the United States Code. Subsection 231(a)(1) would provide that:

> Whoever, in interstate or foreign commerce, by means of the World Wide Web, knowingly makes any communication for commercial purposes that includes any material that is harmful to minors without restricting access to such material by minors pursuant to subsection (c) shall be fined not more than $50,000, imprisoned not more than 6 months, or both.

Subsection 231(a)(2), in turn, would provide for additional criminal fines of $50,000 for "each day" that someone "intentionally violates" § 231(a)(1); and § 231(a)(3) would provide for additional civil fines of $50,000 for "each day" that a person violated § 231(a)(1). Subsection 231(b) would exempt certain telecommunications carriers and other service providers from the operation of § 231(a)(1). Subsection 231(c)(1) would establish what is denominated an "affirmative defense":

> (1) DEFENSE.–It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors –
>
> > (A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; or
> >
> > (B) by any other reasonable measures that are feasible under available technology.

Subsection 231(e) would define, inter alia, the following terms in the criminal

prohibition: (i) "by means of the World Wide Web"; (ii) "commercial purposes"; (iii) "material that is harmful to minors," and "minor." See proposed § 231(e)(1), (2), (6) & (7). In particular, "material that is harmful to minors" would be defined as:

> any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that –
> (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, that such material is designed to appeal to or panders to the prurient interest;
> (B) depicts, describes, or represents, in a patently offensive way with respect to minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals or female breast; and
> (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

The Department's enforcement of a new criminal prohibition such as that proposed in the COPA could require an undesirable diversion of critical investigative and prosecutorial resources that the Department currently invests in combating traffickers in hard-core child pornography, in thwarting child predators, and in prosecuting large-scale and multidistrict commercial distributors of obscene materials. For example, presently the Department devotes a significant percentage of our resources in this area to the highly successful Innocent Images online undercover operation, begun in 1995 by the FBI. 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. To ensure that the initiative remains viable and productive, the Bureau's efforts include the use of new technology and sophisticated investigative techniques, and the coordination of this national investigative effort with other federal agencies that have statutory investigative authority. We also have allocated significant resources for the training of state and local law enforcement agents who must become involved in our effort. To date, the Innocent Images national initiative has resulted in 196 indictments, 75 informations, 207 convictions, and 202 arrests. In addition, 456 evidentiary searches have been conducted.

We do not believe that it would be wise to divert the resources that are used for important initiatives such as Innocent Images to prosecutions of the kind contemplated under the COPA. Such a diversion would be particularly ill-advised in light of the uncertainty concerning whether the COPA would have a material effect in limiting minors' access to harmful materials. There are thousands of newsgroups and Internet relay chat channels on which anyone can access pornography; and children would still be able to obtain ready access to pornography from a myriad of overseas web sites. The COPA apparently would not attempt to address those sources of Internet pornography, and admittedly it would be difficult to do so because restrictions on newsgroups and chat channels could pose constitutional questions, and because any attempt to regulate overseas web sites would raise difficult questions regarding extraterritorial enforcement. The practical or legal difficulty in addressing these considerable alternative sources from which children can obtain pornography raises questions about the efficacy of the COPA and the advisability of expending scarce resources on its enforcement.

Second, such a provision would likely be challenged on constitutional grounds, since it would be a content-based restriction applicable to "the vast democratic fora of the Internet," a "new marketplace of ideas" that has enjoyed a "dramatic expansion" in the

absence of significant content-based regulation. Reno v. ACLU, 117 S. Ct. 2329, 2343, 2351 (1997). As the Court in ACLU suggested, id. at 2341 (discussing Ginsberg v. New York, 390 U.S. 629 (1968)), it may be that Congress could, consistent with the First Amendment, enact an Internet version of a "variable obscenity," harmful-to-minors prohibition, analogous to state-law statutes prohibiting bookstores from displaying to minors certain materials that are obscene as to such minors. See, e.g., American Booksellers v. Webb, 919 F.2d 1493 (11th Cir. 1990), cert. denied, 500 U.S. 942 (1991); American Booksellers Ass'n v. Virginia, 882 F.2d 125 (4th Cir. 1989), cert. denied, 494 U.S. 1056 (1990); Davis-Kidd Booksellers, Inc. v. McWherter, 866 S.W.2d 520 (Tenn. 1993). However, it is not certain how the constitutional analysis might be affected by adaptation of such a scheme from the bookstore context in which it previously has been employed to the unique media of the Internet. Because it may be more difficult for Internet content providers to segregate minors from adults than it is for bookstore operators to do the same, and because the Internet is, in the Court's words, a "dynamic, multifaceted category of communication" that permits "any person with a phone line" to become "a town crier with a voice that resonates farther than it could from any soapbox," ACLU, 117 S. Ct. at 2344, the Court is likely to examine very carefully any content-based restrictions on the Internet.

The decision in ACLU suggests that the constitutionality of an Internet-based "harmful-to-minors" statute likely would depend, principally, on how difficult and expensive it would be for persons to comply with the statute without sacrificing their ability to convey protected expression to adults and to minors. And the answer to that question might depend largely on the ever-changing state of technology, the continuing progress that the private sector makes in empowering parents and teachers to protect minors from harmful material, and the scope and detail of the record before Congress. In this regard, it is notable that the COPA also would establish a Commission (see § 6) to study the ways in which the problem could most effectively be addressed in a time of rapidly evolving technologies. In light of the difficult constitutional issues, we believe that Congress should wait until the Commission has completed its study and made its legislative recommendations before determining whether a criminal enactment would be necessary, and if so, how such a statute should be crafted.

Finally, the COPA as drafted contains numerous ambiguities concerning the scope of its coverage. Such ambiguities not only might complicate and hinder effective prosecution; they also might "render [the legislation] problematic for purposes of the First Amendment," by "undermin[ing] the likelihood that the [bill] has been carefully tailored to the congressional goal of protecting minors from potentially harmful materials." ACLU, 117 S. Ct. at 2344. Among the more confusing or troubling ambiguities are the following:

(a) While the COPA mentions that minors' access to materials on the Internet "can frustrate parental supervision or control" over their children, § 2(1), the only "compelling interest" that the COPA would invoke as a justification for its prohibition is "the protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them," id. § 2(2). The constitutionality of the bill would be enhanced if Congress were to identify as the principal compelling interest the facilitation of parents' control over their children's upbringing, in addition to the government's independent interest in keeping certain materials from minors regardless of their parents' views. See, e.g., ACLU, 117 S. Ct. at 2341 (noting that the statute in Ginsberg presented fewer constitutional problems than the Communications Decency Act because in the former, but not the latter, parents' consent to, or participation in, the communication would avoid application of the statute).

(b) While the bill would not appear to apply to material posted to the Web from outside the United States, that question is not clear; and the extraterritoriality of the prohibition might affect the efficacy and constitutionality of the statute. See ACLU, 117 S. Ct. at 2347 n.45.

(c) It is unclear what difference is intended in separately prohibiting "knowing" violations (proposed § 231(a)(1)) and "intentional" violations (proposed § 231(a)(2)); and there is no indication why the two distinct penalty provisions are necessary or desirable. Moreover, it is not clear, in subsection (a)(1), which elements are modified by the "knowingly" requirement: For example, must the government prove that the defendant knew that the communication contained the harmful-to-minors material? That the defendant knew the materials were, in fact, harmful to minors? Nor is it clear what it would mean, in the context of distribution of the targeted materials over the World Wide Web, to violate subsection (a)(1) "intentionally."

(d) Proposed § 231(a)(3) would provide for civil penalties; but that section does not indicate how such penalties are to be imposed and enforced -- e.g., who would be responsible for bringing civil actions. In this regard, we should note that if Congress were to eliminate criminal penalties altogether, in favor of civil penalties, that would improve the likelihood that the statute eventually would be found constitutional. See, e.g., ACLU, 117 S. Ct. at 2342 (distinguishing the civil penalties upheld in the "indecency" statute at issue in FCC v. Pacifica Foundation, 438 U.S. 726 (1978), from the criminal penalties in the CDA).

(e) The titles of § 3 of the bill, and of proposed § 231 of Title 47, refer to materials "sold by means of the World Wide Web"; and yet the prohibition itself does not appear to prohibit merely the "sale" of harmful material, although it is limited to communications "for commercial purposes."

(f) One of the elements of the basic prohibition in proposed § 231(a)(1) would be that the defendant made the communication "without restricting access to such material by minors pursuant to subsection (c)." Yet subsection (c) itself would provide that such a restriction of access is an affirmative defense. This dual status of the "restricting access" factor appears to create a redundancy; at the very least, it leaves unclear important questions regarding burdens of proof with respect to whether a defendant adequately restricted access.

(g) The COPA definition of "material that is harmful to minors" would be similar to the "variable obscenity" state-law definitions that courts have upheld in cases (cited above) involving restrictions on the display of certain material to minors in bookstores. Those state statutes have, in effect, adopted the "obscenity as to minors" criteria approved in Ginsberg, as modified in accordance with the Supreme Court's more recent obscenity standards announced in Miller v. California, 413 U.S. 15, 24 (1973). But the COPA's definition would, in several respects, be different from the definitions typically used in those state statutes, and the reasons for such divergence are not clear. Is the definition intended to be coterminous with, broader, or narrower than, the standards approved in the cases involving state-law display statutes? The breadth and clarity of the coverage of the COPA's "harmful to minors" standards could have a significant impact on the statute's constitutionality.

(h) Particular ambiguity infects the first of the three criteria for "material that is

harmful to minors," proposed § 231(e)(6)(A). (i) The words "that such material" appear extraneous. (ii) It is unclear whether "is designed to" is supposed to modify "panders to," and, if not, whether the "panders to" standard is supposed to reflect the intended or the actual effect of the expression "with respect to minors." (iii) Which "contemporary community standards" would be dispositive? Those of the judicial district (or some other geographical "community") in which the expression is "posted"? Of the district or local community in which the jury sits? Of some "community" in cyberspace? Some other "community"? Resolution of this question might well affect the statute's constitutionality. See ACLU, 117 S. Ct. at 2345 n.39.

(i) Must the material, taken as a whole, "lack[] serious literary, artistic, political, or scientific value" for all minors, for some minors, or for the "average" or "reasonable" 16-year-old minor? See, e.g., American Booksellers, 919 F.2d at 1504-05 (under a variable obscenity statute, "if any reasonable minor, including a seventeen-year-old, would find serious value, the material is not 'harmful to minors'"); Davis-Kidd Booksellers, 866 S.W.2d at 528 (same); American Booksellers Ass'n, 882 F.2d at 127 (sustaining constitutionality of a state variable obscenity statute after state court had concluded that a book does not satisfy the third prong of the statute if it is "found to have a serious literary, artistic, political or scientific value for a legitimate minority of normal, older adolescents").

(j) In the definition of "engaged in the business" (proposed § 231(e)(2)(B)), it is not clear what is intended by the reference to "offering to make such communications." Also unclear is the effect of the modifier "knowingly" in that same definition's clarification that a person may be considered to be "engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to minors only if the person knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web." Must the person know that the material is posted to the Web? That the material is harmful to minors? That he or she "cause[d]" the material to be posted?

In addition, we have concerns with certain facets of the proposed Commission on Online Child Protection, which would be established under § 6 of the bill. The Commission would be composed of fourteen private persons engaged in business, appointed in equal measures by the Speaker of the House and by the Majority Leader of the Senate, as well as three "ex officio" federal officials (or their designees): the Assistant Secretary of Commerce, the Attorney General and the Chairman of the Federal Trade Commission. The principal duty of the Commission, see § 6(c)(1), would be:

> to conduct a study . . . to identify technological or other methods to help reduce access by minors to material that is harmful to minors on the Internet, [and] which methods, if any--
>
> > (A) that the Commission determines meet the requirements for use as affirmative defenses for purposes of section 231(c) . . . ; or
> >
> > (B) may be used in any other manner to help reduce such access.

If subsection (A) of this provision were construed to permit or to require the Commission to "determine[]," as a matter of law, which methods would satisfy the affirmative defense established in § 231(c), it would violate the constitutional separation of powers because most of the Commission members would be appointed by congressional officials and

would not be appointed in conformity with the Appointments Clause of the Constitution, article II, section 2, clause 2. Accordingly, we would urge deletion of the portion of § 6(c)(1) that follows the word "Internet." For similar reasons, we urge deletion of § 6(d)(4), which would require the Commission, as part of the report it submits to Congress, to describe "the technologies or methods identified by the study that may be used as affirmative defenses for purposes of section 231(c) . . . ." (Even if such a delegation of responsibility to the proposed Commission were otherwise permissible, it would be unwise, in our view, as a matter of policy to permit the Commission – in essence – to make such determinations about a criminal offense.)

Thank you for the opportunity to present our views on this matter. The Office of Management and Budget has advised that there is no objection from the standpoint of the Administration's program to the presentation of this report.

Sincerely,

L. Anthony Sutin
Acting Assistant Attorney General

cc: The Honorable John Dingell
Ranking Minority Member

Mr. GREEN. Do you recall Congress adopting any of these suggestions that were made in this letter that is now in the record or do you have a copy of this letter?

Mr. GERSHEL. I do not, sir.

Mr. GREEN. After reviewing it and looking at what I know about the case, obviously, we made a decision—and, again, we vote for lots of different reasons, but, again, our legislation we pass, we have another branch of government that makes that decision for us. And I may consider something unconstitutional or constitutional, obviously protection against pornography, but they may not be shared by the folks that actually serve on the Supreme Court.

Did DOJ vigorously defend this law before the court that we passed, the Child On-line Protection Act?

Mr. GERSHEL. I believe the Department was very vigorous in its defense of this act both at the district court level and in the Third Circuit in oral argument. I think a review of the government's brief in this matter would demonstrate the strong support we have given to this legislation.

Mr. GREEN. It is my understanding our committee didn't accept the DOJ recommendations. In fact, if you could provide us in later information to us what you know on that—again, that was our decision not to accept those, but, again, you know, we were well aware, at least from this letter, that there were things in that act. I voted for it. I may very well have been a cosponsor of it because of my concern.

Mr. Chairman, I would also like to put in the record something we pulled off the Internet at the FBI library, is available. Again, I talked with my own local agents in Houston, and it is a Parents Guide to Internet Safety.

As I said earlier, I would like to ask unanimous consent to place this in the record because not only the Justice Department but also the Law Enforcement Agency of the FBI is trying to do with Inter-

net safety. And, again, as a parent, it is important to us and someday be a grandparent.

If I could ask unanimous consent to put the Parents Guide to Internet Safety into the record.

Mr. LARGENT. Without objection.

Mr. GREEN. Thank you, Mr. Chairman.

[The information referred to follows:]

A Parent's Guide to Internet Safety

Dear Parent:

Our children are our Nation's most valuable asset. They represent the bright future of our country and hold our hopes for a better Nation. Our children are also the most vulnerable members of society. Protecting our children against the fear of crime and from becoming victims of crime must be a national priority.

Unfortunately the same advances in computer and telecommunication technology that allow our children to reach out to new sources of knowledge and cultural experiences are also leaving them vulnerable to exploitation and harm by computer-sex offenders.

I hope that this pamphlet helps you to begin to understand the complexities of on-line child exploitation. For further information, please contact your local FBI office or the National Center for Missing and Exploited Children at 1-800-843-5678.

Louis J. Freeh, Director
Federal Bureau of Investigation

While on-line computer exploration opens a world of possibilities for children, expanding their horizons and exposing them to different cultures and ways of life, they can be exposed to dangers as they hit the road exploring the information highway. There are individuals who attempt to sexually exploit children through the use of on-line services and the Internet. Some of these individuals gradually seduce their targets through the use of attention, affection, kindness, and even gifts. These individuals are often willing to devote considerable amounts of time, money, and energy in this process. They listen to and empathize with the problems of children. They will be aware of the latest music, hobbies, and interests of children. These individuals attempt to gradually lower children's inhibitions by slowly introducing sexual context and content into their conversations.

There are other individuals, however, who immediately engage in sexually explicit conversation with children. Some offenders primarily collect and trade child-pornographic images, while others seek face-to-face meetings with children via on-line contacts. It is important for parents to understand that children can be indirectly victimized through conversation, i.e. "chat," as well as the transfer of sexually explicit information and material. Computer-sex offenders may also be evaluating children they come in contact with on-line for future face-to-face contact and direct victimization. Parents and children should remember that a computer-sex offender can be any age or sex the person does not have to fit the caricature of a dirty, unkempt, older man wearing a raincoat to be someone who could harm a child.

Children, especially adolescents, are sometimes interested in and curious about sexuality and sexually explicit material. They may be moving away from the total control of parents and seeking to establish new relationships outside their family. Because they may be curious, children/adolescents sometimes use their

on-line access to actively seek out such materials and individuals. Sex offenders targeting children will use and exploit these characteristics and needs. Some adolescent children may also be attracted to and lured by on-line offenders closer to their age who, although not technically child molesters, may be dangerous. Nevertheless, they have been seduced and manipulated by a clever offender and do not fully understand or recognize the potential danger of these contacts.

This guide was prepared from actual investigations involving child victims, as well as investigations where law enforcement officers posed as children. Further information on protecting your child on-line may be found in the National Center for Missing and Exploited Children's *Child Safety on the Information Highway* and *Teen Safety on the Information Highway* pamphlets.

What Are Signs That Your Child Might Be At Risk On-line?

Your child spends large amounts of time on-line, especially at night.

Most children that fall victim to computer-sex offenders spend large amounts of time on-line, particularly in chat rooms. They may go on-line after dinner and on the weekends. They may be latchkey kids whose parents have told them to stay at home after school. They go on-line to chat with friends, make new friends, pass time, and sometimes look for sexually explicit information. While much of the knowledge and experience gained may be valuable, parents should consider monitoring the amount of time spent on-line.

Children on-line are at the greatest risk during the evening hours. While offenders are on-line around the clock, most work during the day and spend their evenings on-line trying to locate and lure children or seeking pornography.

You find pornography on your child's computer.

Pornography is often used in the sexual victimization of children. Sex offenders often supply their potential victims with pornography as a means of opening sexual discussions and for seduction. Child pornography may be used to show the child victim that sex between children and adults is "normal." Parents should be conscious of the fact that a child may hide the pornographic files on diskettes from them. This may be especially true if the computer is used by other family members.

Your child receives phone calls from men you don't know or is making calls, sometimes long distance, to numbers you don't recognize.

While talking to a child victim on-line is a thrill for a computer-sex offender, it can be very cumbersome. Most want to talk to the children on the telephone. They often engage in "phone sex" with the children and often seek to set up an actual meeting for real sex.

While a child may be hesitant to give out his/her home phone number, the computer-sex offenders will give out theirs. With Caller ID, they can readily find out the child's phone number. Some computer-sex offenders have even obtained toll-free 800 numbers, so that their potential victims can call them without their parents finding out. Others will tell the child to call collect. Both of these methods result in the computer-sex offender being able to find out the child's phone number.

Your child receives mail, gifts, or packages from someone you don't know.

As part of the seduction process, it is common for offenders to send letters, photographs, and all manner of gifts to their potential victims. Computer-sex offenders have even sent plane tickets in order for the child to travel across the country to meet them.

Your child turns the computer monitor off or quickly changes the screen on the monitor when you come into the room.

A child looking at pornographic images or having sexually explicit conversations does not want you to see it on the screen.

Your child becomes withdrawn from the family.

Computer-sex offenders will work very hard at driving a wedge between a child and their family or at exploiting their relationship. They will accentuate any minor problems at home that the child might have. Children may also become withdrawn after sexual victimization.

Your child is using an on-line account belonging to someone else.

Even if you don't subscribe to an on-line service or Internet service, your child may meet an offender while on-line at a friend's house or the library. Most computers come preloaded with on-line and/or Internet software. Computer-sex offenders will sometimes provide potential victims with a computer account for communications with them.

What Should You Do If You Suspect Your Child Is Communicating With A Sexual Predator On-line?

1. Consider talking openly with your child about your suspicions. Tell them about the dangers of computer-sex offenders.

2. Review what is on your child's computer. If you don't know how, ask a friend, coworker, relative, or other knowledgeable person. Pornography or any kind of sexual communication can be a warning sign.

3. Use the Caller ID service to determine who is calling your child. Most telephone companies that offer Caller ID also offer a service that allows you to block your number from appearing on someone else's Caller ID. Telephone companies also offer an additional service feature that rejects incoming calls that you block. This rejection feature prevents computer-sex offenders or anyone else from calling your home anonymously.

4. Devices can be purchased that show telephone numbers that have been dialed from your home phone. Additionally, the last number called from your home phone can be retrieved provided that the telephone is equipped with a redial feature. You will also need a telephone pager to complete this retrieval.

5. This is done using a numeric-display pager and another phone that is on the same line as the first phone with the redial feature. Using the two phones and the pager, a call is placed from the second phone to the pager. When the paging terminal beeps for you to enter a telephone number, you press the redial button on the first (or suspect) phone. The last number called from that phone will then be displayed on the pager.

6. Monitor your child's access to all types of live electronic communications (i.e., chat rooms, instant messages, Internet Relay Chat, etc.), and monitor your child's e-mail. Computer-sex offenders almost always meet potential victims via chat rooms. After meeting a child on-line, they will continue to communicate electronically often via e-mail.

7. Should any of the following situations arise in your household, via the Internet or on-line service, you should immediately contact your local or state law enforcement agency, the FBI, and the National Center for Missing and Exploited Children:

    - Your child or anyone in the household has received child pornography;
    - Your child has been sexually solicited by someone who knows that your child is under 18 years of age;
    - Your child has received sexually explicit images from someone that knows your child is under the age of 18.

If one of these scenarios occurs, keep the computer turned off in order to preserve any evidence for future law enforcement use. Unless directed to do so by the law enforcement agency, you should not attempt to copy any of the images and/or text found on the computer.

What Can You Do To Minimize The Chances Of An On-line Exploiter Victimizing Your Child?

1. Communicate, and talk to your child about sexual victimization and potential on-line danger.

2. Spend time with your children on-line. Have them teach you about their favorite on-line destinations.

3. Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for a computer-sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.

4. Utilize parental controls provided by your service provider and/or blocking software. While electronic chat can be a great place for children to make new friends and discuss various topics of interest, it is also prowled by computer-sex offenders. Use of chat rooms, in particular, should be heavily monitored. While parents should utilize these mechanisms, they should not totally rely on them.

5. Always maintain access to your child's on-line account and randomly check his/her e-mail. Be aware that your child could be contacted through the U.S. Mail. Be up front with your child about your access and reasons why.

6. Teach your child the responsible use of the resources on-line. There is much more to the on-line experience than chat rooms.

7. Find out what computer safeguards are utilized by your child's school, the public library, and at the homes of your child's friends. These are all places, outside your normal supervision, where your child could encounter an on-line predator.

8. Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions.

9. Instruct your children:

   - to never arrange a face-to-face meeting with someone they met on- line;
   - to never upload (post) pictures of themselves onto the Internet or on-line service to people they do not personally know;
   - to never give out identifying information such as their name, home address, school name, or telephone number;
   - to never download pictures from an unknown source, as there is a good chance there could be sexually explicit images;
   - to never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing;
   - that whatever they are told on-line may or may not be true.

Frequently Asked Questions:

My child has received an e-mail advertising for a pornographic website, what should I do?

Generally, advertising for an adult, pornographic website that is sent to an e-mail address does not violate federal law or the current laws of most states. In some states it may be a violation of law if the sender knows the recipient is under the age of 18. Such advertising can be reported to your service provider and, if known, the service provider of the originator. It can also be reported to your state and federal legislators, so they can be made aware of the extent of the problem.

Is any service safer than the others?

Sex offenders have contacted children via most of the major on-line services and the Internet. The most important factors in keeping your child safe on-line are the utilization of appropriate blocking software and/or parental controls, along with open, honest discussions with your child, monitoring his/her on-line activity, and following the tips in this pamphlet.

Should I just forbid my child from going on-line?

There are dangers in every part of our society. By educating your children to these dangers and taking appropriate steps to protect them, they can benefit from the wealth of information now available on-line.

Helpful Definitions:

Internet - An immense, global network that connects computers via telephone lines and/or fiber networks to storehouses of electronic information. With only a computer, a modem, a telephone line and a service provider, people from all over the world can communicate and share information with little more than a few keystrokes.

Bulletin Board Systems (BBSs) - Electronic networks of computers that are connected by a central computer setup and operated by a system administrator or operator and are distinguishable from the Internet by their "dial-up" accessibility. BBS users link their individual computers to the central BBS computer by a modem which allows them to post messages, read messages left by others, trade information, or hold direct conversations. Access to a BBS can, and often is, privileged and limited to those users who have access privileges granted by the systems operator.

Commercial On-line Service (COS) - Examples of COSs are America Online, Prodigy, CompuServe and Microsoft Network, which provide access to their service for a fee. COSs generally offer limited access to the Internet as part of their total service package.

Internet Service Provider (ISP) - Examples of ISPs are Erols, Concentric and Netcom. These services offer direct, full access to the Internet at a flat, monthly rate and often provide electronic-mail service for their customers. ISPs often provide space on their servers for their customers to maintain World Wide Web (WWW) sites. Not all ISPs are commercial enterprises. Educational, governmental and nonprofit organizations also provide Internet access to their members.

Public Chat Rooms - Created, maintained, listed and monitored by the COS and other public domain systems such as Internet Relay Chat. A number of customers can be in the public chat rooms at any given time, which are monitored for illegal activity and even appropriate language by systems operators (SYSOP). Some public chat rooms are monitored more frequently than others, depending on the COS and the type of chat room. Violators can be reported to the administrators of the system (at America On-line they are referred to as terms of service [TOS]) which can revoke user privileges. The public chat rooms usually cover a broad range of topics such as entertainment, sports, game rooms, children only, etc.

Electronic Mail (E-Mail) - A function of BBSs, COSs and ISPs which provides for the transmission of messages and files between computers over a communications network similar to mailing a letter via the postal service. E-mail is stored on a server, where it will remain until the addressee retrieves it. Anonymity can be maintained by the sender by predetermining what the receiver will see as the "from" address. Another way to conceal one's identity is to use an "anonymous remailer," which is a service that allows the user to send an e-mail message repackaged under the remailer's own header, stripping off the originator's name completely.

Chat - Real-time text conversation between users in a chat room with no expectation of privacy. All chat conversation is accessible by all individuals in the chat room while the conversation is taking place.

Instant Messages - Private, real-time text conversation between two users in a chat room.

Internet Relay Chat (IRC) - Real-time text conversation similar to public and/or private chat rooms on COS.

Usenet (Newsgroups) - Like a giant, cork bulletin board where users post messages and information. Each posting is like an open letter and is capable of having attachments, such as graphic image files (GIFs). Anyone accessing the newsgroup can read the postings, take copies of posted items, or post responses. Each newsgroup can hold thousands of postings. Currently, there are over 29,000 public newsgroups and that number is growing daily. Newsgroups are both public and/or private. There is no listing of private newsgroups. A user of private newsgroups has to be invited into the newsgroup and be provided with the newsgroup's address.

Federal Bureau of Investigation
Office of Crimes Against Children
935 Pennsylvania Avenue, NW Room 4127
Washington, D.C. 20535

Telephone (202) 324-3666

Mr. GREEN. With that, I would like to ask unanimous consent to place my own statement in the record, and then I will yield back the balance of my time.

Mr. LARGENT. Without objection. The gentleman yields back.

[The prepared statement of Hon. Gene Green follows:]

PREPARED STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXASMR. CHAIRMAN:

I do not believe that any member of this subcommittee supports the thriving Internet marketplace of obscene images.

I am sure all the witnesses here today are going to provide us with ample evidence of the destructive nature this material can have on individuals and their families.

However, Congress has had a checkered past when we have attempted to limit the spread of this material.

The Supreme Court continues to find fault with our efforts to regulate what they consider "free speech."

Their continued decisions to allow very offensive material to circulate over the Internet has crippled efforts designed to protect our children.

I now believe that Congress should intensify educational programs for parents to teach them about the technology and material available to protect children.

I do want to commend the Department of Justice (DoJ) and the Federal Bureau of Investigation (FBI) for their efforts to catch pedophiles on the Internet.

There is no greater danger to our children then a faceless friend who exists outside the knowledge of a parent. Pedophiles have discovered the Internet as the perfect place to pursue their criminal pleasure.

Their trade in child pornography and other obscene material is a threat to communities across this country. The federal government cannot be in every home, school, and library where people may try to access this illegal material.

I believe we must empower parents to monitor their children's on-line activities.

I have conducted community meeting with the ISP's, phone companies, and the FBI to teach children and parents about what they can do to protect their children.

These highlight the currently available blocking technology and information resources that parents can access free of charge to help protect their children on-line.

Mr. Chairman, it is unfortunate that as we seek to bridge the "digital divide" we are actually making it easier for obscene material to flow into our communities like never before.

I appreciate the Chairman holding this hearing and I look forward to the panel discussions.

Mr. LARGENT. I want to thank Mr. Gershel for your attendance, for your patience, and it is my understanding that there is just a couple of follow-up questions, and we are done. And I would just like to reiterate, and correct me if I am wrong, the Justice Department doesn't need the Child On-line Protection Act to prosecute obscenity; is that correct? You were prosecuting obscenity prior to——

Mr. GERSHEL. That is correct.

Mr. LARGENT. Whatever the Third Circuit does is irrelevant in terms of prosecuting obscenity, be it on the Internet or anywhere else; is that correct?

Mr. GERSHEL. That is correct.

Mr. LARGENT. Neither does it need the CDA. You were prosecuting—we have testimony here in the ACLU versus Reno that says the Justice Department itself communicated its view that it was not necessary, CDA, that is. It was prosecuting on-line obscenity child pornography and child solicitation under existing laws and would continue to do so.

Mr. GERSHEL. That is correct.

Mr. LARGENT. So the whole debate over the Child On-line Protection Act, CDA is irrelevant in terms of the job the Justice Department or is not doing on obscenity; is that correct?

Let me ask this one other question, Mr. Gershel. How do you feel when the obscenity industry says and refers to the oversight that you are giving, the prosecution that you are giving and the industry refers to you as having a benign neglect of the industry?

Mr. GERSHEL. Obviously, I would take exception with that. I don't agree with that. We are—we continue to go after and investigate major distributors. I think over time we will have success there. These cases take time. While I may not have the numbers right now to satisfy this committee, I do know from working with the section that there are cases under investigation that we believe satisfy the guidelines and parameters we have established for the investigation and prosecution of obscene pornographers.

Mr. LARGENT. I would like to ask also for—if you have those guidelines written down—you mentioned earlier about the Department had guidelines. I would like to see those guidelines.

And, finally, you mentioned an effort with the local law enforcement agencies, and yet we had testimony on the previous panel that indicated that prior to 1994, 1993, that there was a vigorous effort by the Los Angeles Police Department conducting raids in the San Fernando Valley and that that had virtually come to a stop in the last 5 to 6 years. Do you have a comment on that?

Mr. GERSHEL. To back up to your first question on the guidelines, they are published in the United States Attorneys Manual, Mr. Chairman. I would be happy to get you a copy of those guidelines.

Second, while I can't speak to the L.A. Experience, I have no firsthand knowledge of that, I do know from firsthand experience both in the district where I come from and in my experience here thus far that there is a partnership with State and local. They are involved in these cases. We are working with them.

It is not unusual at all for many State cases to go through the Federal system. It is not unusual, for example, for State prosecutors to become Special Assistant U.S. Attorneys, to prosecute those cases in Federal court. It is not unusual for Federal prosecutors to be cross-designated as local district attorneys for prosecution of State cases. So there is this cross-pollination going on back and forth every day as it concerns these matters.

So, again, I can't speak to the L.A. Experience, but it is certainly a very positive working relationship I believe we have today with State and local entities.

Mr. LARGENT. Concerning the fact that about, some people estimate, 2,000 new sex videos are produced in the San Fernando Valley every month, that might be something you want to look into.

I will yield for a brief question from the gentleman from Mississippi.

Mr. GREEN. Mr. Chairman, I thought it was customary——

Mr. LARGENT. I didn't know you had another question.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. Gershel, one of my frustrations I guess—and if you share it with me—is that as Justice Stewart said one time he knows what obscenity is when he sees it. It is just hard to define it. Does the fuzziness of the definition of obscenity make it more difficult for prosecutions to stick? And also I can understand why it is easier oftentimes to prosecute child pornography because that is not sub-

ject to some of those fuzziness definitions. Can you share your feelings on that with us?

Mr. GERSHEL. Every Federal prosecutor, Congressman, is taught from day one that he or she is not to engage in a prosecution unless he or she believes a substantial likelihood of success on the merits. That is an appropriate burden for prosecutors to have. When it comes to the examination and review of cases dealing with obscenity, prosecutors are required to review that material and make a determination on their own whether or not they believe that material would, in fact, violate whatever community standards this case would be interfacing with.

That is a difficult burden. People might differ on that. We might all find certain material very distasteful. We all know, though, that all pornography is not obscenity. Pornography per se is not illegal unless it is obscene. Prosecutors have to engage in that kind of analysis every time they look at a case dealing with obscenity.

So, yes, it is a challenge. It is difficult. We might disagree on that, but that prosecutor has to be satisfied in his or her mind that that case will pass muster with the jury beyond a reasonable doubt. It is a hard burden.

Mr. GREEN. Is that generally the process the DOJ has—I assume that is in their manual—on whether prosecution should be pursued? Is that generally what you do?

Mr. GERSHEL. That is the policy of the Justice Department in every case that we undertake.

Mr. GREEN. Thank you, Mr. Chairman. I yield back.

Mr. LARGENT. I thank the gentleman.

I yield to the gentleman from Mississippi for a final question, and we will finish the hearing.

Mr. PICKERING. For the panel and for my friend from Texas, just let the record show, between 1989 and 1995 the Justice Department's Child Exploitation and Obscenity section had 126 convictions, prosecutions and convictions of obscenity, not child pornography but just slowly targeting obscenity and $24 million in fines and forfeitures. The problem that I think we are dealing with is, it seems to be around 1995 and after, the Justice Department changed their policy and their priorities with—in relation to obscenity.

So just to follow up on that, Mr. Gershel, in your testimony you say we do investigate and prosecute transmission of obscenity over the Internet, but then you have a very important qualifier, "where appropriate". Since 1996, can you name one case or how many cases you found it appropriate during this period of tremendous explosion of obscenity and pornography and child pornography—since 1996, how many cases have you found it appropriate—given the fact that you had over 126 convictions before 1995, how many have you had since 1996?

Mr. GERSHEL. I believe in the written statement, Congressman, I cited some specific cases. But I should also indicate, again without meaning any disrespect for that same time period, the number of convictions for child pornography, people engaging in that activity, trafficking with children has exploded. In 1999 alone, 525 convictions—an increase of a hundred convictions from the previous year.

Mr. PICKERING. Mr. Gershel, let me again try to find common ground. It seems like you are losing—you are fighting a losing battle on child pornography. You are doing—you are fighting hard. You are doing all you can on child pornography, but it seems like your strategy is not working. The situation is getting worse, not better. Would you reconsider having a dual front, dual effort where you emphasize equally both obscenity and child pornography? Would you consider a change in strategy, a change in policy, and then can Congress help you implement a new policy where you equally emphasize obscenity as well as child pornography?

Mr. GERSHEL. Congressman, I have some difficulty with the premise of the question because there is suggestion that, given the explosion of child pornography, how successful have we really been. I would like to answer that, first, two ways.

First of all, every conviction we get is one less person engaged in that behavior; and, second, it is difficult to quantify the deterrent impact those convictions have. We don't know, for example, how many people who would have otherwise engaged in that conduct have not.

In terms of the second part of your question, I believe we have a strategy for the prosecution of obscenity cases. It is obviously a strategy the Congressman is not content with and not happy with but——

Mr. PICKERING. Can you name me one prosecution since 1996 of obscenity?

Mr. GERSHEL. I believe I have cited some cases——

Mr. PICKERING. You have not cited one case. Name me one case right now.

Mr. GERSHEL. I can follow up that later to the Congressman with cases that we prosecuted.

Mr. PICKERING. Would it be less than five?

Mr. GERSHEL. I am not going to commit. I don't know.

Mr. PICKERING. Versus 126? If industry calls your approach benign neglect——

Mr. GERSHEL. Congressman, our priorities are where they ought to be today I believe.

Mr. PICKERING. What if I could help you have dual emphasis, try a new approach, would you consider that?

Mr. GERSHEL. If you have suggestions and you would like to make suggestions to the Justice Department, we are more than willing to entertain those suggestions and look at them, that I assure you.

Mr. PICKERING. You would be willing—the Justice Department would be willing to consider, if Congress made it a higher priority and gave you the resources to do so, that you would target both obscenity and child pornography?

Mr. GERSHEL. No. I agree we would engage in a dialog with the Congressmen to see what the strategy is.

Mr. PICKERING. The signals you are sending right now are very disturbing. And, with that, let me yield back my time.

Mr. LARGENT. I thank the gentleman.

Again, thank you for your patience. Thank you for your attendance. The hearing is concluded.

[Whereupon, at 1:20 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

STEVE LARGENT
1ST DISTRICT, OKLAHOMA

WASHINGTON OFFICE:
426 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-3601
(202) 225-2211
FAX: (202) 225-9187

DISTRICT OFFICE:
2424 E. 21ST STREET, SUITE 510
TULSA, OK 74114-1741
(918) 749-0014
FAX: (918) 749-0781

Congress of the United States
House of Representatives
Washington, DC 20515–3601

COMMITTEE ON COMMERCE
SUBCOMMITTEES:
ENERGY AND POWER
TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION
FINANCE AND HAZARDOUS MATERIALS

June 8, 2000

Chairman W.J. "Billy" Tauzin
2183 Rayburn House Office Building

Dear ~~Chairman~~ Billy Tauzin:

Enclosed is a copy of a follow up letter from a number of Republican Members of the Telecommunications, Trade and Consumer Protection Subcommittee. I request this be placed in the official record of the hearing. I am also enclosing a copy of President Clinton's Working Group on Unlawful Conduct on the Internet, also to be submitted for the record. This document, 63 pages in length, shows that while undertaking unlawful conduct on the Internet, the Administration failed to acknowledge an entire section of the federal criminal code dealing with obscene material.

Thank you for your help with this hearing and your leadership on this issue. I appreciate the chance to work with you to stem the onslaught of this illegal material on the Internet.

Sincerely,

Steve

Thanks Billy!

Steve Largent
Member of Congress

STEVE LARGENT
1ST DISTRICT, OKLAHOMA

Congress of the United States
House of Representatives
Washington, DC 20515–3601

June 9, 2000

Ms. Janet Reno
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530-0001

Dear Attorney General Reno:

We are writing in response to testimony presented by Mr. Alan Gershel, Deputy Assistant Attorney General, to the House Commerce Subcommittee on Telecommunications, Trade and Consumer Protection on May 24th, 2000. The title of the hearing, "Obscene Material Available via the Internet," was conducted in order to determine the type of obscene material that is available on the Internet and the Department's record of prosecutions and convictions of the producers and traffickers of such material. We were shocked to find that material readily available on the Internet includes depictions of torture, bestiality, bondage and forced sex of women and teenagers. We were also disappointed that all of our specific questions regarding the Department's record on prosecutions of Internet obscenity were met with unprepared, inadequate, and dilatory answers.

Neither Mr. Alan Gershel nor Mr. Terry Lord, Chief of the Child Exploitation and Obscenity Section who accompanied him, were aware of the names of the major distributors and producers of Internet obscenity, but stated that they 'believed' the Department had such information. We request a list of the names and addresses of the top 20 major producers and distributors of obscenity over the Internet, whether domestic or international, as determined by the Department of Justice and whether cases are pending.

Mr. Gershel testified that prosecutors must determine if a case is worthy of prosecution based upon "substantial likelihood on the merits" that a conviction could be expected. In your opinion Ms. Reno, would depictions of the following material hold a substantial likelihood of being determined obscene and therefore resulting in convictions: torture, electroshock sexual torture, bondage, bestiality (all including teenagers and adult women, some including pregnant women), rape, and gang rape?

As a follow up to that hearing, we again ask the following questions of you and request that you respond within the next 60 days. Please list case names, docket numbers and indictments for each Internet obscenity case prosecuted where the lead charge was an obscenity statute beginning with FY 1996. Please list all convictions of the above mentioned cases and all fines and forfeitures obtained.

PRINTED ON RECYCLED PAPER

In his testimony, Mr. Gershel agreed that the 1998 Child Online Protection Act and the 1996 Communications Decency Act were irrelevant to the Committee's Internet obscenity proceedings, and that there *is* substantial overlap between child pornography and obscenity. He later stated that even if Congress were willing to appropriate millions of dollars to the Department specifically for the prosecution of non-child pornography obscenity cases, the Department would only be willing to "enter into a dialogue," not begin prosecutions. This is unacceptable. If this is indeed the stance of the Department of Justice, such a lack of willingness to prosecute an entire section of the federal criminal code may mark the Clinton Administration for years to come as an administration that was praised by the adult entertainment industry as showing "benevolent neglect" towards the producers and distributors of obscenity, while it *ignored* the plight of thousands of parents and families that have been looking for assistance in protecting our nation from this harmful, illegal material.

Thank you in advance for your timely response.

Sincerely,

Steve Largent, M.C.

Charles "Chip" Pickering, M.C.

James Rogan, M.C.

Michael Oxley, M.C.

Robert Ehrlich, M.C.

Barbara Cubin, M.C.

John Shimkus, M.C.

Cliff Stearns, M.C.

Nathan Deal, M.C.

Paul Gillmor, M.C.

THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET
A Report of the President's Working Group on Unlawful Conduct on the Internet

March 2000

TABLE OF CONTENTS

EXECUTIVE SUMMARY

I. INTRODUCTION

A. Executive Order
B. The Working Group on Unlawful Conduct on the Internet
C. Summary of Strategy

II. POLICY FRAMEWORK AND LEGAL ANALYSIS

A. Understanding the Nature of Unlawful Conduct Involving Computers

1. Computers as Targets
2. Computers as Storage Devices
3. Computers as Communications Tools

B. A Framework for Evaluating Unlawful Conduct on the Internet

1. Online-Offline Consistency
2. Appropriate Investigatory Tools
3. Technology-Neutrality
4. Consideration of Other Societal Interests

C. Promoting Private Sector Leadership

D. Sufficiency of Existing Federal Laws

1. Analysis of Substantive Laws
2. New Investigatory Challenges

III. LAW ENFORCEMENT NEEDS AND CHALLENGES

A. Protecting Computers and Networks

B. Federal Tools and Capabilities

1. Personnel, Equipment, and Training
2. Locating and Identifying Cybercriminals
3. Collecting Evidence

C. State and Local Tools and Capabilities

1. Jurisdiction
2. Interstate and Federal-State Cooperation
3. Resources

D. Legal Authorities: Gaps in Domestic Laws

1. Pen Register and Trap and Trace Statute
2. Computer Fraud and Abuse Act
3. Privacy Protection Act
4. Electronic Communications Privacy Act
5. Telephone Harassment
6. Cable Communications Policy Act

E. Challenges for International Cooperation

1. Substantive International Criminal Law
2. Multilateral Efforts
3. Continuing Need for International Cooperation

IV. THE ROLE OF PUBLIC EDUCATION AND EMPOWERMENT

A. Educating and Empowering Parents, Teachers, and Children

1. Technological Tools
2. Non-technological Tools

B. Educating and Empowering Consumers

1. FTC Initiatives: Using Technology to Educate Consumers
2. Department of Commerce Initiatives
3. FDA's Outreach Campaign
4. SEC's Investor Education Efforts
5. CPSC's Consumer Outreach Efforts

C. Developing Cybercitizens

V. CONCLUSIONS AND RECOMMENDATIONS

APPENDICES

A EXECUTIVE ORDER 13,133
B INTERNET FRAUD
C ONLINE CHILD PORNOGRAPHY
D INTERNET SALE OF PRESCRIPTION DRUGS AND CONTROLLED SUBSTANCES
E INTERNET SALE OF FIREARMS
F INTERNET GAMBLING
G INTERNET SALE OF ALCOHOL
H ONLINE SECURITIES FRAUD
I SOFTWARE PIRACY AND INTELLECTUAL PROPERTY THEFT
J MULTILATERAL EFFORTS

THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET
A Report of the President's Working Group on Unlawful Conduct on the Internet
March 2000

EXECUTIVE SUMMARY

The Internet is rapidly transforming the way we communicate, educate, and buy and sell goods and services. As the Internet's potential to provide unparalleled benefits to society continues to expand, however, there has been an increasing recognition that the Internet can also serve as a powerful new medium for those who wish to commit unlawful acts has also grown.

Unlawful conduct involving the use of the Internet is just as intolerable as any other type of illegal activity. Ensuring the safety and security of those who use the Internet is thus a critical element of the Administration's overall policy regarding the Internet and electronic commerce, a policy that seeks to promote private sector leadership, technology-neutral laws and regulation, and an appreciation of the Internet as an important medium for commerce and communication both domestically and internationally. Indeed, the continued growth and maturation of this new medium depends on our taking a balanced approach that ensures that the Internet does not become a haven for unlawful activity.

"Unlawful activity is not unique to the Internet - but the Internet has a way of magnifying both the good and the bad in our society...[W]hat we need to do is find new answers to old crimes."

Vice President Al Gore

August 5, 1999

For these reasons, the President and Vice President established an interagency Working Group on Unlawful Conduct on the Internet, chaired by the Attorney General, to provide an initial analysis of legal and policy issues surrounding the use of the Internet to commit unlawful acts. Specifically, the Working Group considered (1) the extent to which existing federal laws are sufficient to address unlawful conduct involving the use of the Internet; (2) the extent to which new tools, capabilities, or legal authorities may be needed for effective investigation and prosecution of such conduct; and (3) the potential for using education and empowerment tools to minimize the risks from such conduct.

Consistent with the Administration's overall policy, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- *First*, any regulation of unlawful conduct involving the use of the Internet should be analyzed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner, and in a manner that takes account of other important societal interests, such as privacy and protection of civil liberties;

- *Second*, law enforcement needs and challenges posed by the Internet should be recognized as significant, particularly in the areas of resources, training, and the need for new investigative tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and

- *Third*, there should be continued support for private sector leadership and the development of methods -- such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts -- that educate and empower Internet users to prevent and minimize the risks of unlawful activity.

Prior technological advances -- the automobile, the telegraph, and the telephone, for example -- have brought dramatic improvements for society, but have also created new opportunities for wrongdoing. The same is true of the Internet, which provides unparalleled opportunities for socially beneficial endeavors -- such as education, research, commerce, entertainment, and discourse on public affairs -- in ways that we may not now even be able to imagine. By the same token, however, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, and the unlawful distribution of computer software or other creative material protected by intellectual property rights.

"While the Internet and other information technologies are bringing enormous benefits to society, they also provide new opportunities for criminal behavior."

Attorney General Janet Reno

January 10, 2000

In its analysis of existing federal laws in these and other areas, the Working Group finds that existing substantive federal laws generally do not distinguish between unlawful conduct committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication. For example, laws governing fraud – such as credit card fraud, identity theft, securities fraud, gambling, and unfair and deceptive trade acts or practices – apply with equal force to both online as well as offline conduct. To the extent these existing laws adequately address unlawful conduct in the offline world, they should, for the most part, adequately cover unlawful conduct on the Internet. There may be a few instances, however, where relevant federal laws need to be amended to better reflect the realities of new technologies, such as the Internet.

Despite the general adequacy of laws that define the substance of criminal and other offenses, the Working Group finds that the Internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include: the need for real-time tracing of Internet communications across traditional jurisdictional boundaries, both domestically and internationally; the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for hand-in-glove coordination among various law enforcement agencies; and the need for trained and well-equipped personnel – at federal, state, local, and global levels – to gather evidence, investigate, and prosecute these cases. In some instances, federal procedural and evidentiary laws may need to be amended to better enable law enforcement to meet these challenges.

These needs and challenges are neither trivial nor theoretical. Law enforcement agencies today, for example, are faced with the need to evaluate and to determine the source, typically on very short notice, of anonymous e-mails that contain bomb threats against a given building or threats to cause serious bodily injury. Other scenarios raise similarly significant concerns: If a hacker uses the Internet to weave communications through computers in six different countries to break into an online business' records of customer credit card information, consumer confidence in the security of e-commerce and the Internet may be damaged if law enforcement agencies are unable to cooperate and coordinate rapidly with their counterparts in the other countries to find the perpetrator.

Finally, an essential component of the Working Group's strategy is continued support for private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users so as to minimize the risks of unlawful activity. This Administration has already initiated numerous efforts to educate consumers, parents,

teachers, and children about ways to ensure safe and enjoyable Internet experiences, and those efforts should continue. The private sector has also undertaken substantial self-regulatory efforts – such as voluntary codes of conduct and appropriate cooperation with law enforcement – that show responsible leadership in preventing and minimizing the risks of unlawful conduct on the Internet. Those efforts must also continue to grow. Working together, we can ensure that the Internet and its benefits will continue to grow and flourish in the years and decades to come.

THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET
A Report of the President's Working Group on Unlawful Conduct on the Internet
March 2000

On April 7, 1999, visitors to an online financial news message board operated by Yahoo!, Inc. got a scoop on PairGain, a telecommunications company based in Tustin, California. An e-mail posted on the message board under the subject line "Buyout News" said that PairGain was being taken over by an Israeli company. The e-mail also provided a link to what appeared to be a website of Bloomberg News Service, containing a detailed story on the takeover. As news of the takeover spread, the company's publicly traded stock shot up more than 30 percent, and the trading volume grew to nearly seven times its norm. There was only one problem: the story was false, and the website on which it appeared was not Bloomberg's site, but a counterfeit site. When news of the hoax spread, the price of the stock dropped sharply, causing significant financial losses to many investors who purchased the stock at artificially inflated prices.

Within a week after this hoax appeared, the Federal Bureau of Investigation arrested a Raleigh, North Carolina man for what was believed to be the first stock manipulation scheme perpetrated by a fraudulent Internet site. The perpetrator was traced through an Internet Protocol address that he used, and he was charged with securities fraud for disseminating false information about a publicly traded stock. The Securities and Exchange Commission also brought a parallel civil enforcement action against him. In August, he was sentenced to five years of probation, five months of home detention, and over $93,000 in restitution to the victims of his fraud.

I. INTRODUCTION

The use of new technology to commit traditional crimes, such as securities fraud, is not new. Advances in technology – the advent of the automobile and the telephone, for instance – have always given wrongdoers new means for engaging in unlawful conduct. The Internet is no different: it is simply a new medium through which traditional crimes

can now be committed, albeit through the use of inexpensive and widely available computer and telecommunications systems, and with unprecedented speed and on a far-reaching scale. At the same time, as exemplified by the PairGain case, the tools and capabilities associated with new technologies can in many instances help law enforcement agencies solve such crimes.

How should society, and government in particular, respond to the advent of these new ways of committing traditional crimes? This report responds to a recent Executive Order from the President and sketches the preliminary contours of a legal and policy answer to that question. It provides a foundation and offers a framework for further dialogue among law enforcement officials and policymakers at all levels; members of the business community, trade associations, and the non-profit sector; and members of the public on one of the most important issues we face in response to this powerful new communications medium and our new digital economy.

A. Executive Order 13,133

In August 1999, President Clinton established an interagency Working Group on Unlawful Conduct on the Internet ("Working Group"). Executive Order 13,133 directed the Working Group, under the leadership of the Attorney General, to address the issue of unlawful conduct involving the use of the Internet and to prepare a report with recommendations on:

- The extent to which existing federal laws provide a sufficient basis for effective investigation and prosecution of unlawful conduct that involves the use of the Internet, such as the illegal sale of guns, explosives, controlled substances, and prescription drugs, as well as fraud and child pornography;

- The extent to which new technology tools, capabilities, or legal authorities may be required for effective investigation and prosecution of unlawful conduct that involves the use of the Internet; and

- The potential for new or existing tools and capabilities to educate and empower parents, teachers, and others to prevent or to minimize the risks from unlawful conduct that involves the use of the Internet.

The Executive Order further directed the Working Group to conduct its review in the context of current Administration policy concerning the Internet. That policy includes support for industry self-regulation where possible, support for technology-neutral laws and regulations, and an appreciation of the Internet as an important medium for commerce and free speech both domestically and internationally.1 The full text of the Executive Order appears in Appendix A to this report.

This report responds to the directive of Executive Order 13,133 and sets forth a strategy for responding to unlawful conduct on the Internet and for ensuring a safe and secure online environment. As discussed in greater detail below, the Working Group's proposed strategy consists of a 3-part approach that includes: (a) a framework of policy principles for evaluating the need for Internet-specific laws to prohibit unlawful conduct; (b) recognition of the new and significant investigatory needs and challenges posed by the

Internet; and (c) support for private sector leadership and the development of appropriate technological tools and outreach efforts to educate and empower Internet users to prevent and minimize the risks of unlawful acts facilitated by the Internet.

Part II of this report focuses on the first component of the strategy, describing the nature of unlawful activity on the Internet and proposing a framework for analyzing policy and legal responses to such activity. Part II also discusses efforts to promote private-sector leadership in this area and summarizes the Working Group's analysis of the adequacy of existing substantive federal laws, as applied to unlawful conduct on the Internet. Part III of the report then identifies several areas in which new technology tools, capabilities, or legal authorities may be required for effective evidence-gathering, investigation, and prosecution of unlawful conduct that involves the use of the Internet. Part IV of the report focuses on the third component of the strategy, urging support for expanded educational efforts and technological tools to empower Internet users. Finally, Part V summarizes the report's conclusions and recommendations for further action.

B. The Working Group on Unlawful Conduct on the Internet

Pursuant to Executive Order 13,133, the Working Group included the Attorney General, who served as chair of the Working Group; the Director of the Office of Management and Budget; the Secretary of the Treasury; the Secretary of Commerce; the Secretary of Education; the Director of the Federal Bureau of Investigation; the Director of the Bureau of Alcohol, Tobacco and Firearms; the Administrator of the Drug Enforcement Administration; the Chair of the Federal Trade Commission; and the Commissioner of the Food and Drug Administration. In addition, given their interest and expertise in the subject matter, representatives from the Consumer Product Safety Commission, the U.S. Customs Service, the Department of Defense, the Department of State, the National Aeronautics and Space Administration, the National Commission on Libraries and Information Science, the Postal Inspection Service, the U.S. Secret Service, and the Securities and Exchange Commission also participated on the Working Group.

In preparing this report, the Working Group benefitted from the views of representatives of a variety of entities outside the federal government, including, for example:

- State and local groups, such as the National Association of Attorneys General; the National District Attorneys Association; the National Association of Boards of Pharmacies; and the National League of Cities;

- Industry groups, such as the Internet Alliance, the Computer Systems Policy Project, the Business Software Alliance, and representatives of Internet service providers and other high-technology companies; and

- Non-profit advocacy and civil liberties groups, such as the National Center for Missing and Exploited Children, the Center for Democracy and Technology, and the Electronic Privacy Information Center.

We look forward to continuing our dialogue with these and other groups on the important and substantial issues raised in this report.

C. Summary of Strategy

The Internet already is and will continue to be a major force for communication and economic growth in the decades ahead. Consistent with its 1997 *Framework for Global Economic Commerce*, the Administration is continuing to work toward providing a market-oriented policy environment to support the development of this new digital economy. In developing such an environment, it is essential to address some of the possible negative side effects associated with this new economy. These goals are not inconsistent; rather, they are mutually reinforcing: continued growth in economic commerce will require a stable, predictable legal environment that includes vigorous enforcement of consumer protections; and focused law enforcement efforts in turn will promote greater consumer confidence and trust in the Internet as a safe and secure medium of communications and commerce.

To further these goals, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- *First*, evaluating the need for Internet-specific regulation of unlawful conduct through a framework of general policy principles, including the principle that online and offline conduct should be treated consistently and in a technology-neutral way;

- *Second*, recognizing the significant law enforcement needs and challenges posed by the Internet, particularly in the areas of resources, training, and the need for new investigatory tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and

- *Third*, supporting continued private sector leadership and the development of methods -- such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts -- that educate and empower Internet users so as to prevent and minimize the risks of unlawful activity.

Each of these components is an integral part of our overall proposed strategy and is discussed in greater detail in the report that follows.

II. POLICY FRAMEWORK AND LEGAL ANALYSIS

There can be little doubt that the Internet -- a global electronic network of computer networks (including the World Wide Web) that connects people and information 2 -- has revolutionized and will continue to revolutionize how we communicate, educate ourselves, and buy and sell goods and services. The Internet has grown from 65 million users in 1998 to over 100 million users in the U.S. in 1999, or half the country's adult population; the number of Internet users in the U.S. is projected to reach 177 million by the end of 2003; and the number of Internet users worldwide is estimated to reach 502 million by 2003. 3 Business-to-business electronic commerce totaled over $100 billion in 1999 (more than doubling from 1998) and is expected to grow to over $1 trillion by 2003. 4

There can also be little doubt that the Internet provides immeasurable opportunities for far-reaching social benefits. Communications over the Internet, for example, permits unparalleled opportunities for education, research, commerce, entertainment, and discourse on public affairs. Electronic mail ("e-mail") has become an entirely new medium for business and personal communications, allowing users a fast and inexpensive way to keep in touch, to send text, pictures, or sound files to individuals or to groups, and to buy and sell goods and services. News and other information can be made available to anyone with a computer and a modem virtually instantaneously, and more information (on an absolute scale) can be made available to more people, due to the open and decentralized nature of the Internet (anyone can put up a website and "publish" information for the world to see). Access to research databases, directories, encyclopedias, and other information sources previously available only to those with the time, money, and energy to obtain physical access to print material has opened up a world of information to the average citizen. And by making transactions of all kinds cheaper, faster, interactive, and hence more efficient, electrnoic commerce ("e-commerce") is transforming the way businesses operate and the way consumers work, shop, and play.

The Internet, like most new technologies, is an inherently value-neutral tool: It can be used in ways that are socially beneficial or socially harmful. New technologies can, of course, create new forms of socially undesirable behavior. More often, they provide new ways of committing traditionally undesirable behavior. For example, the advent of the telephone allowed innovative lawbreakers not only to develop new crimes (e.g., long-distance toll fraud), but also to commit traditional crimes in a new manner (e.g., harassment through the use of the telephone).

The Internet has fared no better than other technologies against resourceful and technologically sophisticated individuals who seek to commit unlawful acts. Last year, for example, tens of thousands of computer users were struck by "Melissa" and "Explore.Zip.Worm," e-mail viruses that quickly spread around the world, erasing files, crashing systems, and costing companies millions of dollars in support and downtime. More recently, some of the most popular consumer and commercial websites were temporarily disabled as a result of "distributed denial-of-service" attacks. Other websites have been the targets of "page-jacking" schemes, in which websites and search engines are manipulated to drive unsuspecting users to unwanted (usually "adult") websites (see Appendix B for further discussion of page-jacking).

More generally, individuals who wish to use a computer as a tool to facilitate criminal activity may find the Internet as appealing, if not more so, as they did the telephone decades ago or the telegraph before that. Similar to the technologies that have preceded it, the Internet provides a new tool for wrongdoers to commit crimes, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, or the unlawful distribution of computer software or other creative material protected by intellectual property rights. In the most extreme circumstances, cyberstalking and other criminal conduct involving the Internet can lead to physical violence, abductions, and molestation. Although the precise extent of unlawful conduct involving the use of computers is unclear, 5 the rapid growth of the Internet and e-commerce has made such unlawful conduct a critical priority for legislators, policymakers, industry, and law enforcement agencies.

A. Understanding the Nature of Unlawful Conduct Involving Computers

Although definitions of computer crime may differ, not every crime committed with a computer is a computer crime. For example, if someone steals a telephone access code and makes a long distance call, the code they have stolen is checked by a computer before the call is processed. Even so, such a case is more appropriately treated as "toll fraud," not computer crime. Although this example may seem straightforward, many cases cannot be so neatly categorized. For example, a bank teller who steals a $10 bill from a cash drawer is embezzling. A bank teller who writes a computer program to steal pennies from many accounts (at random) and to funnel that money into another bank through the electronic funds transfer system may also be embezzling, but both committing and prosecuting this offense may require a working knowledge of the bank's computer system. Thus, such a crime may reasonably be characterized as a computer offense.

Broadly speaking, computers can play three distinct roles in a criminal case. First, a computer can be the target of an offense. This occurs when conduct is designed to take information without authorization from, or cause damage to, a computer or computer network. The "Melissa" and "Explore.Zip.Worm" viruses, along with "hacks" into the White House and other websites, are examples of this type of offense. Second, a computer can be incidental to an offense, but still significant for law enforcement purposes. For example, drug traffickers may store transactional data (such as names, dates, and amounts) on computers, rather than in paper form. Third, computers can be a tool for committing an offense, such as fraud or the unlawful sale of prescription drugs over the Internet. Each of these three roles can be and often are present in a single criminal case. Although this report focuses primarily on this third category of computer crime, it is important to understand the range of unlawful conduct that involves computers to appreciate the context of law enforcement needs and challenges relating to such conduct.

1. Computers as Targets

One obvious way in which a computer can be involved in unlawful conduct is when the confidentiality, integrity, or availability of a computer's information or services is attacked. This form of crime targets a computer system, generally to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server. Many of these violations involve gaining unauthorized access to the target system (i.e., "hacking" into it).

Offenses involving theft of information may take a variety of forms, depending on the nature of the system attacked. Sensitive information stored on law enforcement and military computers offers a tempting target to many parties, including subjects of criminal investigations, terrorist organizations, and foreign intelligence operatives.

Hackers also target non-governmental systems to obtain proprietary or other valuable information. For example, a hacker might gain access to a hotel reservation system to steal credit card numbers. Other cases may fall into the broad category of intellectual property theft. This includes not only the theft of trade secrets, but also much more

common offenses involving the unauthorized duplication of copyrighted materials, especially software programs. Other cases may involve a perpetrator who seeks private information about another individual, whether as a means to an end (e.g., to extort money or to embarrass the victim through public disclosure), to obtain a commercial advantage, 6 or simply to satisfy personal curiosity. Targets in this category include systems containing medical records, telephone customer records (such as call records or unlisted directory information), or consumer credit report information.

Computers can also be the target of an offense in cases where an offender gains unauthorized access to a system. For instance, an offender may use his computer to break into a telephone switching system (including a private system, such as a PBX) to steal long-distance calling services. (This type of telephone equipment manipulation is often referred to as "phone phreaking" or simply "phreaking.") In some cases, hackers have used the resources of compromised systems to perform intensive computational tasks such as cracking encrypted passwords stolen from other sites. The theft-of-service offenses are often associated with the practice of "weaving," in which a hacker traverses multiple systems (and possibly multiple telecommunications networks, such as the Internet or cellular and landline telephone networks) to conceal his true identity and location. In this scenario, the sole reason for breaking into a given computer may be to use it as a stepping-stone for attacks on other systems.

A more insidious type of damage takes place in cases where the attacker compromises a system in furtherance of a larger scheme. The most well-known examples of this type of attack have involved telephone network computers. In one case, a hacker manipulated telephone switching equipment to guarantee that he would be the winning caller in several call-in contests held by local radio stations. The fruits of his scheme included two sports cars and $30,000 in cash. Internet-connected computers are subject to similar types of attacks. Routers – which are computers that direct data packets traveling on the Internet – are analogous to telephone switches and thus are tempting targets for skilled hackers who are interested in disrupting, or even rerouting, communications traffic on the network.

In the category of attacks known collectively as "denial of service," the objective is to disable the target system without necessarily gaining access to it. One technically straightforward method of accomplishing this objective is "mailbombing," the practice of sending large volumes of e-mail to a single site (or user account) to clog the mail server or even to cause the target host to crash. Other methods – ranging from simply tying up incoming phone lines to more sophisticated attacks using low-level data transmission protocols – may also be used to achieve the same end: rendering the target system unavailable for normal use. These sorts of denial-of-service attacks recently received much publicity when several major websites, including Yahoo.com, Amazon.com, eBay.com, and Buy.com, were temporarily disabled as a result of such attacks.

2. Computers as Storage Devices

A second way in which computers can be used to further unlawful activity involves the use of a computer or a computer device as a passive storage medium. As noted above, drug dealers might use computers to store information regarding their sales and customers. Another example is a hacker who uses a computer to store stolen password

lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software). As discussed in Part III below, computers often can provide valuable evidence that may help law enforcement respond to unlawful conduct.

Indeed, computers have made it possible for law enforcement agencies to gather some information that may not have been previously even maintained in the physical world. For example, an unsophisticated offender, even after "deleting" computer files (as opposed to destroying paper records), might leave evidence of unlawful activity that a trained computer forensic expert could recover. In addition, because an average computer with several gigabytes of memory can contain millions of pages of information, a law enforcement agent might, pursuant to lawful authority (such as a warrant), find volumes of information in one place. Of course, that information is only useful if there are trained computer experts on hand in a timely fashion, familiar with the relevant computer hardware or software configuration, to search the computer for specific information and to retrieve it in readable form (see generally Part III.B below).

3. Computers as Communications Tools

Another way that a computer can be used in a cybercrime is as a communications tool. Many of the crimes falling within this category are simply traditional crimes that are committed online. Indeed, many of the examples in this report deal with unlawful conduct that exists in the physical, "offline" world – the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography. These examples are, of course, only illustrative; online facilities may be used in the furtherance of a broad range of traditional unlawful activity. E-mail and chat sessions, for example, can be used to plan or coordinate almost any type of unlawful act, or even to communicate threats or extortion demands to victims (see cyberstalking box).

Cyberstalking

Cyberstalking is a prime example of the use of computers and the Internet to facilitate a traditional, offline crime. Cyberstalking generally refers to the use of the Internet, e-mail, or other electronic communications devices to "stalk" another person -- where "stalking" in the traditional sense means to engage in repeated harassing or threatening behavior (such as following a person, appearing at a person's home or workplace, making harassing telephone calls, or leaving written messages or objects) that places the victim in reasonable fear of death or bodily injury, cf. 18 U.S.C. § 2261A (prohibiting interstate stalking).

The Internet provides new avenues for would-be stalkers to pursue their victims. For example, in April 1999, a 50-year-old former security guard pled guilty (under California law) to one count of stalking and three counts of solicitation of sexual assault for using the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant impersonated the victim in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized about being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the victim's door saying they wanted to rape her. The defendant faces up to six years in prison.

In August 1999, in response to a request from the Vice President, the Attorney General issued a report, Cyberstalking: A New Challenge for Law Enforcement and Industry (available at

www.usdoj.gov/criminal/cybercrime), exploring the nature of cyberstalking, analyzing the adequacy of current federal and state laws, and recommending ways to improve efforts against cyberstalking. The conclusions of that report track the primary conclusions of this report -- although existing laws (in most instances) may cover the unlawful conduct at issue, the use of the Internet presents numerous investigatory challenges (e.g., those relating to jurisdiction and anonymity) that need to be addressed. The report also found that industry must continue to take an active role in educating and protecting online users against Internet-facilitated unlawful conduct.

Just as legitimate use of the Internet is growing, so too is the Internet increasingly being used to facilitate traditional offenses. For example, because e-mail allows private communications between parties, individuals have used the Internet to send threatening e-mails (including threats to the President). The Internet's one-to-many broadcast capability has also allowed individuals to falsely advertise goods on the Internet or on a website.

The Internet's file transfer capability also enables the Internet to be used as a product delivery system. Because large files can be copied and transmitted reliably, quickly, and cheaply, software companies are now selling software over the Internet: the buyer simply provides a credit card number and downloads the software from the Internet to his or her personal computer. This same capability unfortunately allows for the unauthorized reproduction and distribution of copyrighted software.

Some criminal activities employ both the product delivery and communications features of the Internet. For example, pedophiles may use the Internet's file transfer utilities to distribute and receive child pornography, and use its communications features to make contact with children. Because users need not transmit their voice or appearance, it is easy for an adult to pose as a child and to gain the confidence of children online.

As noted above, this report's primary focus is on this third way in which computers can be used to commit unlawful acts – the use of computers and modern telecommunications facilities as tools (analogous to the use of telephones as tools) to commit an offense. Many of the enforcement and investigative challenges associated with unlawful conduct on the Internet, however, extend to all three ways in which computers can be used for unlawful activity. Consequently, the recommendations contained in this report, if acted upon, could assist law enforcement agencies in combating all types of unlawful conduct involving the use of the Internet.

B. A Framework for Evaluating Unlawful Conduct on the Internet

In its assessment of the extent to which existing federal laws are sufficient to address unlawful conduct involving the use of the Internet, the Working Group developed four general principles to guide its analysis. These principles form the basis for the analytical framework proposed by the Working Group for evaluating the need, if any, for Internet-specific regulation of the particular conduct at issue. The principles flow from the Administration's overall pursuit of policies that recognize and support the enormous potential economic and social benefits of the medium, without unintentionally stifling its growth.

1. Online-Offline Consistency

First, substantive regulation of unlawful conduct (e.g., legislation providing for civil or criminal penalties for given conduct) should, as a rule, apply in the same way to conduct in the cyberworld as it does to conduct in the physical world. If an activity is prohibited in the physical world but not on the Internet, then the Internet becomes a safe haven for that unlawful activity. Similarly, conduct that is not prohibited in the physical world should not be subject to prohibition merely because it is carried out in cyberspace.

Thus, the first step in any analysis of unlawful conduct involving the use of the Internet is to examine how the law treats the same conduct in the offline world. That is, unlawful conduct involving the use of the Internet should not be treated as a special form of conduct outside the scope of existing laws. For example, fraud that is perpetrated through the use of the Internet should not be treated any differently, as a matter of substantive criminal law, from fraud that is perpetrated through the use of the telephone or the mail. To the extent existing laws treat online and offline conduct inconsistently, they should be amended to remove inconsistencies. 7 As the discussion below and the detailed analyses of several examples in the appendices to this report illustrate, however, existing substantive law is generally sufficient to cover unlawful conduct involving the use of the Internet.

2. Appropriate Investigatory Tools

Second, to enforce substantive laws that apply to online conduct, law enforcement authorities need appropriate tools for detecting and investigating unlawful conduct involving the Internet. For example, as discussed in greater detail below, to the extent existing investigative authority is tied to a particular technology, it may need to be modified or clarified so that it also applies to the Internet.

Indeed, new technologies may justify new forms of investigative authority. Before the invention of the telephone, for example, law enforcement had no need for wiretaps, but once it was clear that the telephone was being used to facilitate illegal activity, that new authority – circumscribed with protections for civil liberties and other societal interests – became necessary and appropriate. Similarly, features of the Internet that make it different from prior technologies may justify the need for changes in laws and procedures that govern the detection and investigation of computer crimes. These features, highlighted here in summary form, are discussed in greater detail below:

• *The global and boundaryless nature of the Internet* means that different law enforcement agencies in different jurisdictions will have to cooperate and coordinate their activities in ways that they have probably never before done.

• *Anonymity* on the Internet can provide social benefits, but misrepresentation of identity can also facilitate fraud and deception. Misrepresentation of identity can also result in access by children to inappropriate material and can create law enforcement investigatory challenges, especially if perpetrated by sophisticated computer users, for it can make criminal activity on the Internet more difficult to detect and prove.

• *The potential to reach vast audiences easily* means that the scale of unlawful conduct involving the use of the Internet is often much wider than the same conduct in the offline

world. To borrow a military analogy, use of the Internet can be a "force multiplier."

• *The routine storage of information that can be linked to an individual* can often provide more information to law enforcement (where an individual has been identified or a computer lawfully seized) than may be available in the offline world, but only if the electronic information is handled properly by a trained investigator and if the information obtained is ultimately available in useable form.

Thus, apart from ensuring that online and offline behavior is treated consistently as a matter of substantive law, legislators and policymakers should examine whether law enforcement agencies have appropriate tools to detect and investigate unlawful conduct involving the Internet. That is, even if Internet-specific laws are unnecessary to ensure that criminal and civil penalties apply to the use of the Internet to facilitate unlawful conduct, it may be necessary to alter or augment law enforcement's tools and authorities to meet the new investigatory challenges that such unlawful conduct presents.

3. Technology-Neutrality

Third, to the extent specific regulation of online activity may be necessary (in view of the consistency principle noted above), any such regulation should be drafted in a technology-neutral way. Regulation tied to a particular technology may quickly become obsolete and require further amendment. In particular, laws written before the widespread use of the Internet may be based on assumptions regarding then-current technologies and thus may need to be clarified or updated to reflect new technological capabilities or realities. For example, regulation of "wire communications" may not account for the fact that communications may now occur through wireless means or by satellite. Technology-specific laws and regulations may also "lock-in" a particular technology, hindering the development of superior technology.

4. Consideration of Other Societal Interests

Fourth, any government regulation of conduct involving the use of the Internet requires a careful consideration of different societal interests. In addition to society's strong interests in investigating and prosecuting unlawful conduct, society also has strong interests in promoting free speech, protecting children, protecting reasonable expectations of privacy, providing broad access to public information, and supporting legitimate commerce.

As applied to the Internet, consideration of other societal interests can present difficult issues, in part because the Internet is different in important ways from existing, "traditional" modes of communication. For example, the Internet is a multi-faceted communications medium that allows not only point-to-point transmission between two parties (like the telephone), but also the widespread dissemination of information to a vast audience (like a newspaper). Internet-specific laws and policies that operate by analogy to those designed for telephone communications or the press may not fit the new medium. The Internet also presents new issues relating to online expectations of privacy and confidentiality that may or may not have analogs in the offline world. Accordingly, rules and regulations designed to protect the safety and security of Internet users should be carefully tailored to accomplish their objectives without unintended consequences,

such as stifling the growth of the Internet or chilling its use as a free and open communication medium.

Another aspect of the need to consider different societal interests is to appreciate the need for an appropriate balance among the roles of the government (whether federal, state, local, or other) and the role of the private sector in formulating solutions to Internet policy issues. For example, because regulation of the practices of medicine and pharmacy has traditionally been the province of the states, regulation of online pharmacies presents difficult federal-state jurisdictional and coordination issues (see Appendix D). And, as discussed in the next section, given the Administration's support for private-sector leadership and market-based self-regulation regarding e-commerce, there must be ongoing and regular dialogue with interested parties and groups to ensure that government policies do not have unintended consequences.

C. Promoting Private Sector Leadership

Consistent with the Administration's overall e-commerce policy, the private sector has a critical role to play in ensuring a safe and secure online environment. The distributed, networked, and decentralized nature of the Internet now means that the "rules of the road" must be global, flexible, effective, and readily adaptable to technological change. In particular, the private sector must take the lead in areas such as the design of new technologies to protect children online, self-regulatory consumer protection initiatives, and coordination and cooperation with law enforcement authorities.

In response to the marketplace, for example, there are now many technological options for shielding children from inappropriate content. As discussed in more detail in Part IV.A below, these technological developments include filtering and blocking software, outgoing information blocks, filtered Internet browsers and search engines, filtered Internet service providers, time blocking mechanisms and monitoring tools. Similarly, child-friendly websites are now widespread on the Internet. These websites allow parents to limit a child's access to sites beyond the web service designated for the child's use. In July 1999, the private sector launched the "GetNet Wise" initiative, a new easy-to-access online resource for parents to help keep their children safe online. "GetNet Wise" is a resource containing information on Internet safety tips, consumer content filtering products, law enforcement contacts, and a guide to quality educational and age appropriate online content. Although none of these tools can guarantee that a child will be shielded at all times from inappropriate material on the Internet, their use gives parents the ability to restrict a child's use to the resources on the Internet that they may deem appropriate.

In addition, in response to challenges issued by Commerce Secretary Daley, industry has worked with consumer representatives to develop consumer protection practices, codes of conduct for business-to-consumer e-commerce, and alternative, easy-to-use mechanisms for consumer resolution, redress, and enforcement.

- For example, the Better Business Bureau's online division, BBBOnLine, is working with industry, consumer, and government representatives to develop a voluntary code to provide online merchants with guidelines to implement consumer protections. The code includes guidance on key consumer

protections such as disclosure of sale terms, data privacy, dispute resolution mechanisms, and non-deceptive advertising.

• Another group, the Electronic Commerce and Consumer Protection Group, whose members include America Online, American Express, AT&T, Dell, IBM, Microsoft, Time Warner, Inc., and Visa, is working with consumer leaders to develop an innovative approach to jurisdiction as it applies to consumer protection in a global electronic marketplace. This group is also developing a voluntary code of conduct. The goal of the group is to formulate concrete approaches to protect consumers and facilitate e-commerce.

These creative efforts are important to developing effective consumer protection in e-commerce, because as e-commerce expands to encompass more international business-to-consumer transactions, the traditional means of protecting consumers solely through national laws will become more difficult.

In addition to specific consumer protection initiatives, the private sector's dedication and support for a secure Internet system is crucial to curbing unlawful conduct on the Internet. Not only must industry continue to develop security policies and safeguards for their networks and systems, but it should also continue its efforts to identify security flaws that threaten the Internet. For example, computer experts from industry and the Computer Emergency Response Team Coordination Center of Carnegie-Mellon University recently warned of a new Internet security threat that wrongdoers could potentially use to place malicious programs on a victim's computer and to gather information that a person volunteers on websites, such as credit card and Social Security numbers. 8 The Partnership for Critical Infrastructure Protection will provide a cross-sectoral forum for the private sector to address a variety of infrastructure assurance issues, including information sharing, development of best practices, promotion of needed R&D, and workforce development. Another example of private sector cooperation in this effort is InfraGard, which is an information sharing and analysis partnership among the FBI, private sector companies, academic institutions, and other federal, state, and local agencies. InfraGard serves to increase the security of the national infrastructure through ongoing exchanges of infrastructure-protection information and through education, outreach, and other awareness efforts.

The private sector also has a key role to play in continuing to coordinate and cooperate with law enforcement authorities as appropriate. Industry trade groups, such as the Internet Alliance and the Information Technology Association of America ("ITAA"), have been working to develop public-private cooperative efforts that will mutually benefit law enforcement, industry, and consumers. The Internet Alliance's Law Enforcement and Security Council has been developing parental control software and educational campaigns, opening channels of communication between industry and law enforcement representatives, and creating training programs for law enforcement and industry on issues of mutual interest. ITAA, through its Cybercitzen Project (see Part IV.C below), is working with the Department of Justice to develop education campaigns, personnel exchange programs, and a directory of industry contacts.

Although the private sector has taken important steps in the areas of prevention and

online security, there is still much that industry can do to ensure that the Internet is a safe and secure environment. For example:

• Industry should continue to develop and embrace initiatives to protect consumers and children online. These may include technological tools (e.g., more sophisticated blocking, filtering, and parental control software) as well as non-technological tools (e.g., educational campaigns). In particular, industry should continue to be involved in education programs that teach younger Internet users about online responsibilities and online citizenship.

• Industry should continue to cooperate with law enforcement agencies as appropriate. This does not mean that industry ought to be a "co-regulator" with government or that industry needs to be an online police officer. But it does mean that industry should be a voluntary, responsible partner in society's fight against crime, educating its employees on how to recognize unlawful conduct on the Internet and what to do if they discover such conduct. It means working with law enforcement agencies to develop reliable and efficient procedures and channels of communication and cooperation for processing law enforcement requests and investigative information. As the "Melissa" virus case demonstrates, industry's involvement and reporting of information is often crucial to the investigation and prosecution of online offenders.

• Industry should carefully balance reasonable expectations of customer privacy with the need to ensure a safe and secure online environment. For example, some industry members may not retain certain system data long enough to permit law enforcement to identify online offenders. This does not mean that data retention policies need to be uniform or mandatory. To the contrary, in evaluating the costs and benefits of data retention – which include a wide variety of considerations, including market needs, protection of consumer privacy, and public safety – industry should simply give appropriate weight to the wider value to itself and to society of retaining certain information that, among other things, may be essential to apprehending a lawbreaker.

• Industry should be encouraged to recognize that meaningful self-regulation is in its interest as well as in the interests of its customers. Information technology security programs (that teach employees about computer ethics, responsible online practices, and security policies), for instance, help protect computer systems from intruders as well as online offenders. Indeed, as we noted at the outset of this report (see Part I.C above), law enforcement and industry share a common mission in reducing unlawful online conduct, for a safe and secure online environment is essential to consumer confidence, which is in turn essential to ensuring that the Internet continues to grow as a medium for communications and commerce.

The Working Group looks forward to continuing to work with the private sector and other interested parties and groups in partnership on these important issues.

D. Sufficiency of Existing Federal Laws

Private sector leadership is, of course, necessary but not sufficient to address unlawful conduct involving the use of the Internet. Substantive criminal laws represent a societal determination, expressed through our democratic institutions of government, that certain conduct is so harmful or morally unacceptable that reliance on self-regulation or the market to regulate the conduct is inappropriate. There is thus a need to evaluate whether existing substantive laws apply to unlawful conduct that is committed through the use of the Internet.

Toward that end, and in the context of the framework of policy principles discussed above, the Working Group analyzed several examples of unlawful conduct involving the use of the Internet. The examples, as discussed in detail in appendices to this report, include not only those specifically mentioned in Executive Order 13,133, but also those taken from our experience with legislative proposals and from Executive branch agencies that have jurisdiction to respond to these forms of unlawful conduct.

1. Analysis of Substantive Laws

The Working Group's analysis reveals that existing substantive federal laws appear to be generally adequate to protect users from unlawful conduct on the Internet. As listed and summarized in Table 1 below, such laws generally do not distinguish between unlawful conduct committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication.

For example, laws governing fraud – such as credit card fraud, identity theft, securities fraud, and unfair and deceptive trade acts or practices – apply with equal force to both online as well as offline conduct (see Appendix B). Laws prohibiting the distribution and possession of child pornography and the luring of minors across state lines for unlawful sexual activity have been used with success to prosecute and convict those who use the Internet to distribute such material or to communicate with child victims in violation of statutory prohibitions (see Appendix C). And laws that prohibit the dispensing of prescription drugs without a valid prescription from a licensed medical professional can be applied to online pharmacies that dispense prescription drugs without required regulatory safeguards (see Appendix D).

Laws in other areas – the sale of firearms (Appendix E); interstate transmission of gambling information (Appendix F); sale of alcohol (Appendix G); securities fraud (Appendix H); and theft of intellectual property (Appendix I) – also generally apply to online conduct as well as offline conduct. Although existing federal laws generally prohibit Internet gambling, technological advances make it prudent to update existing federal laws to ensure that they are technology-neutral and prohibit gambling activities that did not exist before the advent of the Internet (see Appendix F). And, in the area of intellectual property protection, current Sentencing Guidelines pertaining to intellectual property crimes should be updated to ensure that law enforcement agencies and prosecutors commit the resources to continue to pursue these cases vigorously (see Appendix I).

Table 1 – Summary of Analysis of Existing Federal Law

Types of Unlawful Conduct	Examples of Potentially Applicable Federal Laws	Detailed Discussion in Appendix
Internet Fraud	15 U.S.C. §§ 45, 52 (unfair or deceptive acts or practices; false advertisements) 15 U.S.C. § 1644 (credit card fraud) 18 U.S.C. §§ 1028,1029,1030 (fraud in connection with identification documents and information; fraud in connection with access devices; and fraud in connection with computers) 18 U.S.C. § 1341 et seq. (mail, wire, and bank fraud) 18 U.S.C. § 1345 (injunctions against fraud) 18 U.S.C. § 1956, 1957 (money laundering)	B
Online Child Pornography, Child Luring, and Related Activities	18 U.S.C. § 2251 et seq. (sexual exploitation and other abuse of children) 18 U.S.C. § 2421 et seq. (transportation for illegal sexual activity)	C
Internet Sale of Prescription Drugs and Controlled Substances	15 U.S.C. § 45 et seq. (unfair or deceptive acts or practices; false advertisements) 18 U.S.C. § 545 (smuggling goods into the United States) 18 U.S.C. § 1341 et seq. (mail, wire, and bank fraud; injunctions against fraud) 21 U.S.C. § 301 et seq. (Federal Food, Drug, and Cosmetic Act) 21 U.S.C. §§ 822, 829, 841, 863, 951-971 (Drug Abuse Prevention and Control)	D
Internet Sale of Firearms	18 U.S.C. § 921 et seq. (firearms)	E
Internet Gambling	15 U.S.C. § 3001 et seq. (Interstate Horseracing Act) 18 U.S.C. § 1084 (transmission of wagering information) 18 U.S.C. §§ 1301 et seq. (lotteries) 18 U.S.C. § 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises)	F

	18 U.S.C. § 1953 (interstate transportation of wagering paraphernalia) 18 U.S.C. § 1955 (prohibition of illegal gambling businesses) 28 U.S.C. §§ 3701-3704 (professional and amateur sports protection)	
Internet Sale of Alcohol	18 U.S.C. § 1261 et seq. (liquor traffic) 27 U.S.C. §§ 122, 204 (shipments into states for possession or sale in violation of state law)	G
Online Securities Fraud	15 U.S.C. § 77e, 77j, 77q, 77x, 78i, 78j, 78l, 78o, 78ff (securities fraud)	H
Software Piracy and Intellectual Property Theft	17 U.S.C. § 506 (criminal copyright infringement) 17 U.S.C. § 1201 et seq. (copyright protection and management systems) 18 U.S.C. § 545 (smuggling goods into the United States) 18 U.S.C. §§ 1341, 1343 (frauds and swindles) 18 U.S.C. § 1831 et seq. (protection of trade secrets) 18 U.S.C. §§ 2318-2320 (trafficking in counterfeit labels for phonorecords, copies of computer programs or computer program documentation or packaging, and copies of motion pictures or other audio visual works)	I

2. New Investigatory Challenges

As law enforcement agencies adapt to a more technology-based society, they need to be aware of the challenges, as well as the benefits, of online investigations. In certain circumstances, law enforcement agencies have available to them tools and capabilities created by the Internet and computers that can assist them in their fight against computer-facilitated unlawful conduct. For example, just as advances in telephone technology gave law enforcement agents the ability to determine the origin of fraudulent or threatening calls, the Internet has given law enforcement agencies the ability to find unsophisticated offenders who leave the equivalent of "fingerprints" as they commit unlawful acts. Indeed, someone who makes a threat in an Internet chat room to set off a bomb at a school and who makes little or no effort to hide his or her identity (e.g., where accurate identifying information exists for a particular "screen name") can often be traced and found with relative ease.

At the same time, law enforcement agencies must also acknowledge the growing sophistication of other computer users, who wear the equivalent of Internet gloves that may hide their fingerprints and their identity. The following is an overview of

investigatory challenges -- taken from actual experiences involving online investigations and discussed in greater detail in the appendices for each example of Internet-facilitated unlawful conduct -- that law enforcement agencies must consider as they become more proficient with such investigations.

(a) *Jurisdiction*

In the physical world, one cannot visit a place without some sense of its geographic location. Whether a particular street address or an area of the world, human travel is spatially based. By contrast, because one can access a computer remotely without knowing where, in physical space, that computer is located, many people have come to think of the collection of worldwide computer linkages as "cyberspace" (a term coined by science fiction writer William Gibson). In short, cybercriminals are no longer hampered by the existence of national or international boundaries, because information and property can be easily transmitted through communications and data networks.

As a result, a criminal no longer needs to be at the actual scene of the crime (or within 1,000 miles, for that matter) to prey on his or her victims. Just as telephones were (and still are) used by traditional boiler-room operators to defraud victims from a distance, a computer server running a webpage designed to defraud senior citizens might be located in Thailand, and victims of the scam could be scattered throughout numerous different countries. A child pornographer may distribute photographs or videos via e-mail running through the communications networks of several countries before reaching the intended recipients. Likewise, evidence of a crime can be stored at a remote location, either for the purpose of concealing the crime from law enforcement and others, or simply because of the design of the network. 9 To be sure, the Internet increases the ability of law enforcement officials and others to detect and gather evidence from a distance. For example, a website used in a fraud scheme can be spotted from an agent's office, whereas detecting a fraudulent telemarketing or mail-fraud scheme might well require extensive field work. Long-distance detection, however, may take the investigation and prosecution of these crimes out of the exclusive purview of any single jurisdiction, thereby creating yet other challenges and obstacles to crime-solving.

For example, a cyberstalker in Brooklyn, New York may send a threatening e-mail to a person in Manhattan. If the stalker routes his communication through Argentina, France, and Norway before reaching his victim, the New York Police Department may have to get assistance from the Office of International Affairs at the Department of Justice in Washington, D.C. which, in turn, may have to get assistance from law enforcement in (say) Buenos Aires, Paris, and Oslo just to learn that the suspect is in New York. In this example, the perpetrator needs no passport and passes through no checkpoints as he commits his crime, while law enforcement agencies are burdened with cumbersome mechanisms for international cooperation, mechanisms that often derail or slow investigations. With scores of Internet-connected countries around the world, the coordination challenges facing law enforcement are tremendous. And any delay in an investigation is critical, as a criminal's trail often ends as soon as he or she disconnects from the Internet.

This does not mean that traditional legal structures cannot be meaningfully applied to the Internet. Even though connections may be of short duration, computers are still

physically located in particular places. The challenge to law enforcement is identifying that location and deciding which laws apply to what conduct. The question is how sovereign nations can meaningfully enforce national laws and procedures on a global Internet.10

Inconsistent substantive criminal laws are only part of the problem, for investigative techniques are also controlled by national (or local) law. For example, law enforcement agencies must consider such issues as transborder execution of search warrants. If law enforcement agents in the United States access a computer and seize data from a computer, the fact that they have a search warrant makes that action lawful. If, with that same search warrant, they remotely access a Canadian computer (from the United States), might this constitute a criminal act under Canadian law notwithstanding the existence of the U.S. warrant? To the extent that agents know nothing more than an Internet protocol address (essentially, a series of numbers that identify a particular machine), the physical location of the computer to be searched may not be accurately known. Yet ignorance of physical location may not excuse a transborder search; consider how we would react to a foreign country's "search" of our defense-related computer systems based upon a warrant from that country's courts.

This transborder issue may raise domestic issues as well. Gambling and obscenity laws provide criminal sanctions for individuals based, in part, upon their location. One federal law prohibits transmitting information assisting in the placing of bets or wagers on sporting events or contests unless both the sender and receiver are in states or foreign countries where gambling is legal, see 18 U.S.C. §1084. Obscenity laws are also typically interpreted in light of local community standards, cf. Miller v. California, 413 U.S. 15 (1973). Even the search warrant provision in the federal rules requires that agents seek a warrant in the district where the property to be seized is located, see Fed. R. Crim. P. 41 (a). To the extent the location of the sender, recipient, or data is unknown and perhaps unknowable, it may be difficult for law enforcement to investigate and prosecute online offenders.

(b) *Identification*

Another thorny issue stems from the lack of identification mechanisms on global networks, and the fact that individuals can be anonymous or take on masked identities (i.e., adopt false personas by providing inaccurate biographical information and misleading screen names). Simply stated, given the current state of technology, it can be difficult to accurately identify an individual (especially sophisticated users who take affirmative steps to hide their identity) on the Internet. As noted above, there are cases, such as the PairGain case, where law enforcement agencies have been able to track down online criminals who leave evidence of their unlawful conduct. Over time, the ability of criminals to use technology to evade identification and the ability of law enforcement to use technology to overcome such evasion will continue to evolve. Some of the challenges of identifying perpetrators of unlawful conduct on the Internet, as well as measures taken by law enforcement and the private sector 11 to respond to such challenges, are discussed below in Part III of this report.

At the very least, there needs to be widespread and extensive training of law enforcement personnel in ways to identify those who use the Internet to commit unlawful acts.

Moreover, as policymakers increasingly seek to protect certain classes of citizens, most notably minors, from unsuitable material (e.g., pornography and gambling), the potential problems of identification are evident. How can activities, such as gambling or the sale of prescription drugs or alcohol, be limited to adults when children can identify themselves as adults? Similarly, if adults can falsely identify themselves as children and lure real children into dangerous situations, how can these victims be protected?

These issues are frequently at the heart of legislative and investigative efforts. Although there have been proposals to build identification mechanisms into Internet protocols, such an approach would have to be supported by internationally-recognized, market-based, standards-making bodies whose agenda did not directly include public safety. Even if the market supported such an approach, however, such proposals are controversial, because there are strong reasons to allow anonymity in communications networks. For example, whistleblowers may wish to remain anonymous, as may a group of rape victims who wish to convene an electronic meeting to discuss their experiences without revealing their identities.

In an attempt to create a framework for evaluating identification mechanisms on the Internet, some have compared the Internet with other forms of communications, such as pay telephones and regular mail, which may offer users some degree of anonymity. Of course, the difference between these traditional means of communication and the Internet is significant, and attempting to solve Internet problems only by drawing analogies to existing technologies will often fail. The problem is that the analogies may capture some aspects of the new technology, but fail to capture others. For example, the telephone and mail systems cited above allow predominantly one-to-one communications. Although someone wishing to defame a public figure or harass others can, in theory, call thousands of people anonymously, the time and cost make this impractical. By contrast, the cost-free, simple, one-to-many nature of the Internet dramatically alters the scope and impact of communications. It is this difference which explains why children who would never spend their weekly allowance buying *The Anarchist Cookbook* at a college bookstore may download the same information from the Internet and possibly injure themselves or others testing a recipe for the making of a bomb.12 Given the complexity of this issue, balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead.

(c) *Evidentiary Issues*

Electronic data generated by computers and networked communications such as the Internet can be easily destroyed, deleted, or modified. Digital photographs are but one example of digital information that can be altered in ways that may be difficult to detect. As a result, law enforcement officials must be cognizant of how to gather, preserve, and authenticate electronic evidence. This will not only require substantial training of law enforcement personnel, but also sufficient experience with such evidence by investigators, prosecutors, defense counsel, courts, and others until clear rules and standards are established. The volume of electronic evidence that requires forensic analysis is also increasing substantially. The increasing use of computers and the Internet, of course, often means that information or records of communications that were previously never retained or routinely destroyed can (in some instances) now be recovered, but such recovery may still require sophisticated computer forensics.

Thus, for the reasons noted above, law enforcement agencies face significant challenges in dealing with electronic evidence. These challenges will continue to grow, because electronic evidence can become a part of any investigation. Electronic evidence, for example, can show up as any of the following items, each presenting distinct evidentiary challenges: a drug trafficker's computerized customer records; a digital photograph of a murder scene; an encrypted e-mail containing details of a terrorist plot or fraud scheme; or a system administrator's log files of a hacker attack.

(d) *Infrastructure Protection*

Protecting our information infrastructure is imperative but difficult for a host of reasons: the number of different systems involved, the interdependency of these systems, the varied nature of the threats (physical and cyber, military, intelligence, criminal, natural), and the fact that many of these infrastructures are maintained primarily by the commercial sector. Addressing cyberthreats to our infrastructure is particularly difficult, because of differing views regarding our vulnerabilities; the need to balance interests relating to privacy, economic competitiveness, commercial risk, national security, and law enforcement; and the overlapping authorities within the federal government for dealing with information infrastructure issues. Although such issues are beyond the scope of this report, see National Plan for Information Systems Protection (released Jan. 7, 2000), appreciating the importance and complexity of infrastructure protection is key to understanding the needs of law enforcement in countering unlawful conduct involving the Internet (see Part III.A below).

(e) *Commingling*

The ability of an individual to use one computer to conduct both lawful and unlawful activities or to store both contraband and legally possessed material presents another significant issue. Such commingling defies simple solutions. The fact is, one computer can be used simultaneously as a storage device, a communications device (e.g., to send, store, or retrieve e-mail), and a publishing device. Moreover, that same computer can be used simultaneously for both lawful and unlawful ventures, and the problem becomes more complex when a single machine is shared by many users.

For example, individuals who distribute child pornography or copyrighted software using their home computers may also publish a legitimate newsletter on stamp collecting or use an e-mail service with that same computer. By seizing the computer, law enforcement agencies can stop the illegal distribution of contraband, but may, at the same time, interfere with the legitimate publication of the newsletter and the delivery of e-mail, some of which may be between users who have no connection with the illegal activity. Similarly, a doctor who is illegally prescribing drugs over the Internet may not only have on her computer evidence relating to the illegal prescriptions, but files related to her lawfully treated patients. Likewise, an attorney accused of operating an Internet sportsbook may keep in the same folder on his computer materials relating to his gambling business and documents subject to the attorney-client privilege. Seizure of the doctor's or the lawyer's files in such circumstances could result in the seizure of legally privileged material.

III. LAW ENFORCEMENT NEEDS AND CHALLENGES

As the examples of Internet-facilitated unlawful conduct discussed above and in the appendices illustrate, the increasing sophistication and global reach of such conduct make it all the more important to adequately equip law enforcement agencies at all levels.

The following are some of the principal issues that should be considered when evaluating how to better equip federal, state, and local law enforcement agencies to ensure the safety and security of Internet users. We urge further analysis, in consultation with state and local law enforcement, industry, and privacy and other groups, to determine the most appropriate ways to promote private sector leadership in this area and to empower law enforcement – at all levels – with the needed tools, capabilities, and legal authorities to curb unlawful conduct on the Internet while protecting privacy and supporting the growth of the electronic marketplace.

A. Protecting Computers and Networks

In assessing the tools, capabilities, and legal authorities needed by law enforcement to address unlawful conduct on the Internet, we must consider the larger context of how to protect the systems and networks of this Nation that make our businesses run and operate our Nation's defenses and infrastructure. As we have become more dependent on technology, our energy production and distribution channels, our transportation networks, and our telecommunication systems have become increasingly reliant on a computer-based infrastructure.

Without a protected infrastructure, there could be no conduct, lawful or unlawful, on the Internet. Electronic commerce and the marketplace cannot thrive without a strong infrastructure that the public can trust and rely upon. Consequently, proposals relating to law enforcement challenges in this area (e.g., new investigative tools, capabilities, or legal authorities) need to be assessed in light of the broader need to protect the vital infrastructure, because cyberattacks on infrastructures and other cybercrimes can lead to telecommunications breakdowns that disable electronic commerce and destroy our citizens' confidence in the Internet and computer networks.

The protection of this country's computers and networks requires everyone's cooperation. It demands a partnership among all federal agencies with responsibilities for certain special functions, such as law enforcement, intelligence, and defense.13 It also requires all federal agencies to take appropriate preventive measures to protect their computer systems against attack. Most important, because the overwhelming majority of the Nation's infrastructure is in private hands, the private sector must take the steps necessary to prevent attacks against its systems.14 The Partnership for Critical Infrastructure Protection, which recently held a day-long kickoff meeting, will serve as a key catalyst for this activity. In addition, we must consider the needs of state and local law enforcement, which play a critical role in fighting the cybercriminals on the street.

Meeting its responsibility to protect critical infrastructures is one of the central challenges for law enforcement as we face the 21st Century. As our reliance on the Internet, on automated systems, and on other technological advances increases with every passing month, the potential impact of attacks on critical infrastructure expands as well. Law enforcement needs to be provided the legal mechanisms and financial resources to be

prepared to confront this challenge in partnership with other federal agencies, with the private sector, and with state and local agencies. The Administration recognized this need for unprecedented cooperation between the private and public sectors in Presidential Decision Directive 63. That document provides a framework for federal agencies to cooperate with their private sector partners and for the formation of the National Infrastructure Protection Center, an interagency center for analysis, warning, and investigation of cybercrime. In addition, the Partnership for Critical Infrastructure Protection provides a cross-sectoral forum for the private sector to address a variety of infrastructure assurance issues.

B. Federal Tools and Capabilities

1. Personnel, Equipment, and Training

In 1986, an astronomer-turned-systems-manager at the University of California at Berkeley found a 75-cent accounting error in a computer's billing program, which led to the discovery that an unauthorized user had penetrated Berkeley's computer system. When the astronomer, Clifford Stoll, began to investigate further, he discovered that a hacker identified as "Hunter" was using Berkeley's computer system as a conduit to break into U.S. government systems and steal sensitive military information. The hacker's objective seemed to be to attain U.S. anti-ballistic missile technology.

As he began to pursue the hacker, Stoll encountered serious problems. To begin with, Stoll was unable to find computer-literate law enforcement personnel with an appreciation of the technical nature of the criminal activity. Local and federal agencies that Stoll contacted, including the FBI and CIA, initially expressed little interest in pursuing what at first looked like a computer prank. (Moreover, until government investigators learned of the potential threat to national security, they had no interest in pursuing a case which appeared to have damages valued at less than one dollar.) Because Hunter's trail vanished each time he ended a communication, he could only be traced when he was online. But because it was often after business hours (and, indeed, sometimes in the middle of the night) when Hunter attacked, there were few (if any) law enforcement personnel available during those sessions. The call was eventually traced to Germany, but adding an international element to the case now meant that it was usually after business hours in at least one time zone where the communication was passing through. Stoll cleverly resorted to generating phony official-looking data to keep the hacker interested and online long enough for the trace to be completed. Eventually, the source of the attacks was identified as a German hacker, and he was successfully prosecuted there.[15]

Ironically, one reason this investigation was successful is that Stoll did not rely solely on law enforcement, but instead was able to work directly with telephone company personnel, who in turn worked with other telecommunications providers. His investigation brought to light a number of interdependent personnel and resource requirements that, unless fulfilled, will impede the success of law enforcement in this area. Despite significant progress since the time of this example, it remains a useful illustration of some of the fundamental issues that continue to need further attention at the domestic and international level to eliminate weak links in the chain of an investigation.

(a) *Experts Dedicated to High-tech Crime*

The complex technical and legal issues raised by computer-related crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a firm understanding of computers and telecommunications. The complexity of these technologies, and their constant and rapid change, mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a full-time basis, immersing themselves in computer-related investigations and prosecutions. Many agencies, including the Departments of Justice, Treasury, and others, have already dedicated available resources to do so. The Federal Trade Commission ("FTC") adopted this approach when it formed an Internet Rapid Response Team and successfully halted several online fraud schemes in a matter of weeks. Some federal agency inspectors general have also established computer crime divisions, complete with forensics laboratories and technical experts, and many have information technology audit and inspection capabilities to assist their agencies in identifying vulnerabilities, best practices, and other critical infrastructure issues.

But more of such expertise and the resources to support the increasing cyber-workload are needed. Indeed, each state attorney general's office, each U.S. Attorney's office, each federal law enforcement squad, and each country's equivalent to the U.S. Department of Justice should have a dedicated high-tech crime unit that knows how to respond to a fast-breaking investigation and that knows who else to contact in the chain of a communication and how to reach those individuals. These experts will also be needed to support other law enforcement authorities faced with high-tech issues, such as when a computer is used to facilitate an otherwise traditional crime.

The Department of Justice has designated a prosecutor in each U.S. Attorney's Office to serve as a computer and telecommunications coordinator for that district, and the FBI has established the National Infrastructure Protection Center and the National Infrastructure Protection and Computer Intrusion program. Staffing levels for these programs are below the level needed to effectively address the concerns raised in this report. Given the magnitude of the challenges, the continually changing technology, and the complexity of these investigations, these are necessarily resource-intensive programs.

(b) *Experts Available on a 24-Hour Basis*

A unique feature of high-tech and computer-related crime is that it often requires immediate action to locate and identify criminals. The trail of a criminal may be impossible to trace once a communication link is terminated, because the carrier may not keep (or is not required by law to keep) records concerning each individual communication. This lack of information is due, in part, to the fact that there often is no longer a revenue-related reason for recording transmission information (i.e., connection times or source and destination) for individual connections. For example, many businesses no longer bill their customers by individual telephone call or Internet connection but, instead, by bulk billing (e.g., a single rate for one month of usage). When a carrier does not collect traffic data, a suspect's trail may evaporate as soon as the communication terminates.

Therefore, investigators and prosecutors with expertise in this field must be available 24 hours a day so that appropriate steps can be taken in a fast-breaking high-tech case. For

example, the National Infrastructure Protection Center operates a 24-hour/7-day-a-week command post for around-the-clock coverage of computer intrusion matters. And, Attorney General Reno recently challenged the National Association of Attorneys General to work with the Department of Justice and other appropriate organizations (among other things) to create a 24/7 network of computer crime enforcement personnel in every state.16

(c) *Regular and Frequent Training*

Because of the speed at which communications technologies and computers evolve, and because criminal methods in these areas generally change more rapidly than those in more traditional areas of crime, experts must receive regular and frequent training in the investigation and prosecution of high-tech cases. Programs such as those offered by the FBI at its Quantico facility and elsewhere and under the National Cybercrime Training Partnership provide such training to federal, state, and local law enforcement personnel, but more is needed. Government computer professionals, such as systems operators and administrators, also need regular and frequent training, because they are often the first to detect unlawful conduct that targets federal computer systems.

In addition to domestic training, countries should participate in coordinated training with other countries, so transnational cases can be pursued quickly and seamlessly. By way of example, in the U.S., high-tech prosecutors at the federal level attend a 1-week training course every year, with training provided by both government and private sector personnel. Likewise, in 1998, the G-8 countries held an international high-tech training conference for its countries' law enforcement personnel.

(d) *Up-to-date Equipment*

In the past, a police officer would be given a gun, a flashlight, and a notepad when he or she was hired. Twenty years later, the three items would be returned to the police department when the officer retired, and the only intervening equipment expenses would have had to do with replacement bullets, batteries, and note paper. Today, keeping pace with computer criminals means that law enforcement experts in this field must be properly equipped with the latest hardware and software. Providing proper equipment, however, can be one of the more difficult challenges, because the cost of purchasing and upgrading sophisticated equipment and software places considerable burdens on the budget process.

Ultimately, personnel, training, and equipment needs require the direct involvement of senior officials, such as the Attorney General and FBI Director, because of the budget-request and budget-allocation processes that are involved with such expenditures. Moreover, in many jurisdictions, senior policymakers may not be as familiar with new computer and telecommunications technologies and with threats posed by cybercriminals. If senior government officials in those jurisdictions are unfamiliar with the technologies at issue or the new threats and challenges they pose, they may be hesitant to support law enforcement by seeking appropriate legislative and budgetary changes. The need for adequate personnel, resources, and training is thus a critical issue in this increasingly important area of law enforcement.

Encryption and the Challenge of Unlawful Conduct on the Internet

The practice of encryption, sometimes called cryptography, is the use of mathematical or other methods to hide the content of messages or files. Encryption often uses a secret key — a word, phrase, or other information that is not easily guessed — to ensure that only those who know the key can read the content of the file or message. Cryptography has been studied and practiced by governments and militaries for centuries, but only in the last decade have individuals begun to encrypt large amounts of data using computers. Today, encryption can be used to secure both communications over networks and stored data on computers.

Encryption now presents and will continue to present a challenge to law enforcement confronting Internet-related crime. Robust encryption products make it difficult or impossible for law enforcement to collect usable evidence using traditional methods, such as court-authorized wiretaps and search warrants. Moreover, as encryption tools are increasingly built into retail software and hardware products, the use of encryption will require little skill or effort for users to implement. As a result, lawbreakers can communicate and store information relating to crimes with little fear that police can discover and use that information. Increasing limitations on law enforcement's ability to deter, detect, investigate, and prove certain types of crime may place the public safety at correspondingly increased risk.

By the same token, encryption has many positive aspects which assist in protecting users of the Internet from crime. Companies use encryption to enhance protection of their proprietary data, so that even if their networks are penetrated by a hacker, the information stored on the network will be meaningless to the intruder. Similarly, individuals and merchants use cryptography to help protect sensitive personal data (such as credit card numbers) from being revealed to outsiders during transactions over a network. Finally, in coming years, individuals will use products and services based upon cryptography to ensure that the person or organization with whom they are communicating is authentic, thus reducing fraud and identity theft.

The immediate challenge for law enforcement is finding ways to promote the many positive aspects of encryption while maintaining the current ability to prevent and prosecute crime. To do this, federal, state, and local law enforcement agencies will have to enhance their understanding of encryption tools and develop techniques for obtaining evidence despite their use by criminals. By working with industry, privacy groups, and others, we will continue to look for solutions that harmonize society's interests in protecting privacy and protection from crime.

2. Locating and Identifying Cybercriminals

When a hacker disrupts air traffic control at a local airport, when a cyberstalker sends a threatening e-mail to a public school or a local church, or when credit card numbers are stolen from a company engaged in e-commerce, investigators must locate the source of the communication. To accomplish this, they must trace the "electronic trail" leading from the victim back to the perpetrator. But the realities for law enforcement engaged in such a pursuit are very different from those of just a few years ago. Consequently, society faces significant challenges in the coming years as online criminals become more sophisticated and as technology may make anonymity more easily available. The following are some of the challenges facing both industry and law enforcement.

Divested and Diverse Environment. In today's communications environment, where telecommunication services are no longer provided by a monopoly carrier, a single end-

to-end transmission is often carried by more than one carrier. As a result, the communications of a hacker or other criminal may pass through as many as a dozen (or more) different types of carriers, each with different technologies (e.g., local telephone companies, long-distance carriers, Internet service providers ("ISPs"), and wireless and satellite networks). The communication may also pass through carriers in a number of different countries, each in different time zones and subject to different legal systems. Indeed, each of these complications may exist within a single transmission. This phenomenon makes it more difficult (and sometimes impossible) to track criminals who are technologically savvy enough to hide their location and identity.

Wireless and Satellite Communications. Cellular and satellite-based telephone networks allow users to roam almost anywhere in the world using the same telephone. Although the social and commercial benefits of such networks are obvious, these networks can also provide a valuable communication tool for criminal use. Although sophisticated technology may allow law enforcement, under certain circumstances, to identify the general geographic region from which a wireless call is originating or terminating, the use of such technology raises profound and difficult issues at the intersection of privacy and law enforcement policies. Moreover, even identifying the owner of a particular mobile phone can be difficult, because mobile phones can be altered to transmit false identifying information. As the costs of mobile phones and mobile telephony service drop, we can expect to see the marketing of more "disposable phones," which will further complicate the ability of law enforcement agencies to gather evidence linking a perpetrator to the communication.

Satellite telephony presents additional issues. Current satellite-based networks transmit communications from users through one or more satellites and to earth-based gateways where the communications are routed using land-line systems. Providers of satellite-based telephony services typically do not need to build a gateway in each country to which service is to be provided. Indeed, it may be the case that one or two gateways can service an entire continent. The government's ability to protect the public's safety and privacy can be threatened in instances where a gateway servicing U.S. customers is located outside the U.S. In such cases, the content of the communications, as well as identifying information about the callers themselves, will be subject to the relevant laws (if any) of the host country and may not be protected in the same manner that the information is protected in the United States. More importantly to law enforcement, the location of a gateway in another country makes it difficult for law enforcement to meet its obligation to protect against criminal activities. In addition, law enforcement may have to rely on the willingness and technical and legal ability of the country in which the gateway is located to trace telephone calls, obtain information regarding suspected criminals in the United States, and provide that information to U.S. law enforcement agencies.

Recognizing the benefits and challenges created by advances in global telephony, the federal government has been working with telecommunications companies and foreign law enforcement agencies to ensure that the public interest is served in a global telephony environment. The government is also addressing global telecommunications issues in various international fora to ensure that the U.S. retains its ability to protect the U.S. public's privacy and safety.

Real-time Tracing. Tracing a communication from victim back to attacker may be

possible only when the attacker actually is online. Sophisticated criminals can alter data concerning the source and destination of their communications, or they may use the Internet account of another. In addition, transmission information may not be retained or recorded by communications providers or may not be captured at all or held for only a short period of time. Even if it is generated and retained, it might be deleted by a skilled intruder to hide his identity.

Consequently, when law enforcement officials have information that a crime is being committed online, they often must attempt to trace a communication as it occurs. To do so, a law enforcement agency must know which computer crime expert to call in which jurisdiction, be able to contact the relevant individuals at various ISPs and carriers, and secure appropriate legal orders in each jurisdiction where a relevant carrier or ISP is located. (Notably, many ISPs already coordinate and cooperate with law enforcement agencies in this respect, and industry groups are developing "best practices" to encourage others to do the same.) Critical personnel must also be available when network-facilitated crimes occur after business hours. When these crimes occur across borders, real-time investigations must be able to proceed on an international scale.

Technical Infrastructure and Data Retention. If the communications network and the computers and software that run it have not been designed and configured to generate and preserve critical traffic data, information relating to the source and destination of a cyber-attack will likely not exist. Consider, for example, the use by many ISPs of modem banks to provide Internet access to incoming callers. An ISP may have 2 million customers, but maintain only 100,000 phone lines, based on an expectation that no more than 100,000 customers will ever dial in at any given time. The ISP may give only one access number to its customers and dynamically assign each incoming call to the next available line. Without a revenue-related reason for knowing the specific line used for each connection, the ISP's network may not be designed to generate the data necessary to link a customer with a specific incoming line. This, in turn, may make it impossible to trace the origin of the telephone call into the ISP's network. Such a network design can make it difficult to obtain traffic data critical to an investigation.

Even if a particular piece of the technical infrastructure is capable of generating and preserving needed data, such data are not useful if carriers do not collect and retain such records.17 Issues concerning whether, to what extent, and for how long critical data are retained are decided both by national laws (or the lack thereof) and by industry practices, which generally reflect market preferences and other revenue-related needs.18 In examining data retention practices and laws, careful consideration must be given to privacy concerns, market realities, and public safety needs.

U.S. law enforcement may be significantly affected by the 1995 and 1997 directives of the European Union ("EU") concerning the processing of personal data, including the deletion of traffic data. EU Member States are in the process of developing implementing legislation.19 As the directives are implemented into national legislation throughout the EU, it is vital that public safety be considered, along with the privacy and market force elements.

Anonymity. Anonymous e-mail accounts, which are e-mail accounts where subscriber information is not requested or verified,20 are the proverbial double-edged sword. Such

anonymous accounts can protect privacy, but they add new complexities to identifying online lawbreakers, such as individuals who send child pornography, death threats, computer viruses, or copyright-protected works by e-mail.

Similarly, "anonymous re-mailer" services, which are e-mail services that strip the source address information from e-mail messages before passing them along to their intended recipients, raise difficult privacy and law enforcement policy issues. On the one hand, anonymous re-mailer services provide privacy and encourage freedom of expression. For example, in early 1999, these services allowed ethnic Albanians to provide first-hand accounts of Serbian atrocities in Kosovo without the fear of retribution. On the other hand, such services can plainly frustrate legitimate law enforcement efforts. Indeed, as early as 1996, one such service expressly touted itself as "a way to thwart attempts by intelligence agencies to trace illegal traffic . . . . It holds all incoming messages until five minutes after the hour, then re-mails them in random order. The messages are sent through five to twenty other re-mailers, with a stop in at least one of the several countries noted for lax law enforcement." 21

To be sure, individuals can generally engage in many "real world" activities relatively anonymously, such as making small cash payments and attending public events. But they cannot remain anonymous in other contexts, such as opening a bank account or registering a car. Indeed, many financial institutions have substantial customer identification requirements. As discussed in Part II.B above, Internet-based activities should be treated consistently with physical world activities and in a technology-neutral way to further important societal goals (such as the deterrence and punishment of those who commit money laundering). National policies concerning anonymity and accountability on the Internet thus need to be developed in a way that takes account of privacy, authentication, and public safety concerns.

3. Collecting Evidence

When computers are used to store information, law enforcement agents generally can, upon securing a warrant, search the computer in the same way that they would a briefcase or file cabinet. The difference, of course, is that a computer can store a tremendous amount of information, including evidence that might not be known to the computer's owner. 22 This feature of computer information can, of course, be both a benefit to and a challenge for law enforcement. It can benefit law enforcement by providing information (sometimes in a readily searchable way) that might not have existed in the non-computer world. But it can obviously present law enforcement challenges by highlighting the need for training and expertise (and time) for the information to be recovered. For example, one computer with 3 gigabytes of memory can contain the equivalent of one million pages of information. "Keyword" searches can miss relevant information, and the difficulty of the search and recovery of information may depend on how familiar the forensic expert is with the particular hardware and software configuration of the computer at issue. Moreover, if information on the computer is encrypted, it may be completely inaccessible to law enforcement and contribute little to solving the crime at issue (see box on encryption).

C. State and Local Tools and Capabilities

State and local law enforcement agencies play a significant role in addressing unlawful conduct on the Internet. These agencies have been crucial in combating online child pornography, prescription drug sales, gambling, and fraud. Consequently, any initiatives by the federal government to address unlawful conduct on the Internet must account for the important role state and local governments play in online investigations and prosecutions and should address the following three areas of fundamental concern to these state and local law enforcement authorities: (1)jurisdiction; (2)cooperation and coordination; and (3)resources.

The following is a brief discussion of the jurisdictional, cooperation and coordination, and resources issues facing state and local governments. Because the Executive Order that prompted this report focuses on federal law enforcement issues, we recommend that a more detailed analysis of state and local law enforcement issues be undertaken as a next step.

1. Jurisdiction

In responding to the challenge of law enforcement on the Internet, one of the problems that state and local governments face is that, although the crimes and schemes on the Internet may victimize local populations, the medium over which these crimes are committed permits a defendant to be located anywhere in the world. The traditional investigative tools available to the state – interviews, physical or electronic surveillance, and service of subpoenas for the production of documents or for testimony – are not necessarily adequate to compel information from a wrongdoer who is located out of state.

For example, if a fraud scheme is committed against Ohio residents by an operator of a website located in Florida, and the Ohio prosecutors issue a subpoena for records from the company in Florida, there is currently no formal procedural mechanism for the service and enforcement of that subpoena. Although the Ohio prosecutors may informally succeed in obtaining assistance from the Florida authorities, this is a matter of professional courtesy rather than legal process. There is no guarantee that the subpoena will be served, or, if served, enforced. Running into such a roadblock could well mean the end of the Ohio investigation. In the absence of any ability to investigate the case themselves, it remains possible for the Ohio prosecutors simply to refer the case to their Florida counterparts by reporting their complaints about the cybercriminal in Florida, but if the crime involves no Florida victims or is otherwise outside its jurisdiction, there is no guarantee that the case will be investigated by anyone.

This example illustrates the kinds of jurisdictional hurdles that are becoming increasingly common for state and local law enforcement authorities pursuing crime over the Internet. Another difficulty in this area arises from the disparate approaches taken by state courts to whether a state can exert long-arm jurisdiction over an Internet site accessible in that state. The lack of uniformity may make it more difficult for investigators in some jurisdictions to conduct meaningful investigations of Internet conduct. And, the enforcement of state electronic surveillance orders can also be a challenge. The Internet and modern satellite communications have made it more necessary for state wiretap orders to be served on and enforced against an out-of-state service provider. Unfortunately, no legal mechanism exists that would allow this. For example, drug

traffickers operating entirely in New York, but using satellite telephones with signals that are received at a ground station outside of New York, potentially are completely immune from a New York wiretap order if the out-of-state ground station refuses to comply with a New York court's wiretap order.

2. Interstate and Federal-State Cooperation

Because the gathering of information in other jurisdictions and internationally will be crucial to investigating and prosecuting cybercrimes, all levels of government will need to develop concrete and reliable mechanisms for cooperating with each other. The very nature of the Internet – its potential for anonymity and its vast scope – may cause one law enforcement agency to investigate, inadvertently, the activities of another agency that is conducting an undercover operation. Likewise, the law enforcement agency of one state may require the assistance of another for capturing and extraditing a criminal to its state for prosecution. In other words, crimes that were once planned and executed in a single jurisdiction are now planned in one jurisdiction and executed in another, with victims throughout the United States and the world.

The effective coordination and cooperation between various branches of the law enforcement community is crucial to any effort to combat unlawful conduct on the Internet. One area that may deserve further review concerns the extent to which federal, state, and local authorities can share and gather information about pending cases, potential targets, investigative procedures and tactics, and contact personnel. Such coordination is necessary for federal, state, and local law enforcement agencies to avoid duplicating and possibly undermining investigations.

In January 2000, Attorney General Reno challenged the National Association of Attorneys General and other state and local law enforcement groups to make it a priority to respond to these significant needs. Among other things, she specifically urged the groups to:

- Create a 24-hour cybercrime point of contact network, where each participating federal, state, and local law enforcement agency would provide a designated contact who is available 24 hours per day, 7 days per week to assist with cybercrime issues. This contact could be available via a pager system or coordinated through a centralized "command center."

- Create an online clearinghouse for sharing information to avoid duplication of effort and multiple investigations of the same unlawful conduct. Existing mechanisms, such as XSP, LEO, or Consumer Sentinel, may either serve this function or serve as building blocks for such a service.

- Develop conferences for all state and local Internet investigators and prosecutors, yearly or bi-annually, at which recent developments are discussed, case progress shared, and networks reinforced that will facilitate state, federal, and local cooperation.

- Develop additional policies and mechanisms to enhance cooperative interstate investigative and prosecutorial capacities and encourage

coordination among their constituents.

3. Resources

Although state and local law enforcement organizations are responsible for investigating and prosecuting most forms of unlawful conduct involving the use of the Internet, they have limited resources with which to pay the substantial costs of developing the technical, investigative, and prosecutorial expertise and acquiring the new and often expensive technology necessary to address these crimes. Personnel, equipment, and training must be funded not only once but on a recurring basis. In addition, the structure of state and local law enforcement agencies is different from state to state and even county to county within a state. Resources must not be so restricted as to prohibit a state or local government from tailoring programs and initiatives within their current structures.

Federal funding can be useful in supplementing state and local spending on the necessary personnel, training, and equipment to properly investigate and prosecute high technology crime cases. To the extent that federal funds are expended on enhancing federal law enforcement's forensic capabilities, these projects should be structured in a way that allows state and local law enforcement to use these forensic resources. Regional computer forensic laboratories, such as the new laboratory in San Diego, have been successful and may be a model for other such facilities. 23

D. Legal Authorities: Gaps in Domestic Laws

Law enforcement agencies need strong laws to protect society against unlawful activity. This is as true in the online world as it is in the offline world. As discussed above in Part II and detailed in the appendices to this report, existing federal law is generally adequate to cover unlawful conduct involving the use of the Internet.

Strong substantive laws, however, that apply to the use of the Internet to commit traditional offenses such as fraud, child pornography, gambling, and the illegal sale of intellectual property are necessary but not sufficient to ensure a safe and secure online environment. To achieve that goal, law enforcement, in cooperation with the private sector, must also be able to gather evidence, investigate, and prosecute these cases. Unfortunately, in some areas, the legal authorities and tools needed to do this have lagged behind technological and social changes. This section examines several laws related to the investigation and prosecution of high-tech offenses that have not kept pace with technological changes. Although we do not offer specific solutions in this report, we are committed to working with interested parties to devise appropriate solutions.

1. Pen Register and Trap and Trace Statute

Pen registers (devices that record the numbers dialed on a telephone line) and trap and trace devices (devices that capture incoming electronic impulses that identify the originating number) are important tools in the investigation of unlawful conduct on the Internet. Unfortunately, the statute that governs such devices, 18 U.S.C. §§ 3121-3127, is not technology-neutral and has become outdated.

As an initial matter, advances in telecommunications technology have made the language

of the statute obsolete. The statute, for example, refers to a "device" that is "attached" to a telephone "line," id. § 3127(3). Telephone companies, however, no longer accomplish these functions using physical hardware attached to actual telephone lines. Moreover, the statute focuses specifically on telephone "numbers," id., a concept made out-of-date by the need to trace communications over the Internet that may use other means to identify users' accounts.

Moreover, the deregulation of the telecommunications industry has created unprecedented hurdles in tracing long-distance telephone calls. Many different companies, located in a variety of judicial districts, may handle a single call. Under the existing statute, however, a court can only order communications carriers within its district to provide tracing information to law enforcement. As a result, investigators have to apply for several, sometimes many, court orders to trace a single communication, causing needless waste of time and resources and hampering important investigations.

2. Computer Fraud and Abuse Act

Originally passed in 1984, and amended in 1986, 1994, and 1996, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, protects a broad range of computers that facilitate interstate and international commerce and communications. For example, section 1030(a)(2) makes it a crime to access a computer without or in excess of authority and obtain (1) financial information from a financial institution or credit reporting company; (2) any information in the possession of the government; or (3) any private information where the defendant's conduct involves interstate or foreign commerce. Section 1030(a)(5) makes it a crime for anyone to knowingly cause the transmission of a computer program, information, code, or command, that results in unauthorized damage to a protected computer. (A "protected computer" is one used exclusively or partly by the United States or a financial institution in which the defendant's conduct affects the government's or financial institution's operation of the computer; or any computer that is used in interstate or foreign commerce or communications, see 18 U.S.C. § 1030(e)(2).) 24

Despite its broad reach and relatively recent amendment, the statute nevertheless contains several flaws that could hinder law enforcement's ability to respond effectively to unlawful conduct on the Internet. For example, given the increasing interdependency and availability of global computer networks, it is increasingly likely that computer system intruders within the United States may begin to concentrate their unlawful activity on systems located entirely outside the United States. Alternatively, individuals in foreign countries may route communications through systems located within the United States, even as they hack from one foreign country to another. In such cases, they may hope that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution. It is unclear whether section 1030, in its existing form, protects against such situations, which may affect the United States even though the perpetrator and the victim are located elsewhere.

The Department of Justice has encountered several instances where intruders have attempted to damage critical systems used in furtherance of the administration of justice, national defense, or national security, as well as systems (whether publicly or privately owned) that are used in the provision of "critical infrastructure" services such as telecommunications, transportation, or various financial services, but where proof of

damage in excess of $5,000, as required by section 1030(a)(5), has not been readily available. Although such activities may pose extreme risks to our infrastructure, section 1030(a)(5) currently does not allow law enforcement to proceed without evidence of over $5,000 in damages.

Another problem is that prosecutions under section 1030(a)(5) carry a mandatory minimum sentence of at least six months. In some instances, prosecutors have exercised their discretion and elected not to charge some defendants whose actions otherwise would qualify them for prosecution under that section, knowing that the result would be mandatory imprisonment. It may be useful to examine whether requiring imprisonment for six months should be applied in more limited circumstances than allowed under existing law, or whether other punishments, such as reduced penalties and forfeiture of any instrumentalities or proceeds of the violation, might provide adequate punishment and deterrence.

3. Privacy Protection Act

The Privacy Protection Act of 1980 ("PPA"), 42 U.S.C. §2000aa, et seq., makes it unlawful for local, state, or federal law enforcement authorities to "search for or seize any work product materials" or any "documentary materials . . . possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication," 42 U.S.C. § 2000aa(a), (b) (emphasis added). The statute defines "work product materials" as materials prepared or possessed in anticipation of communicating such materials to the public, except if the materials constitute contraband or the fruits or instrumentalities of crime. Id. § 2000aa-7(b). "Documentary materials," on the other hand, consist of materials upon which information is recorded, once again with the exception of contraband and the fruits or instrumentalities of crime. Id. § 2000aa-7(a).

In enacting the PPA, Congress restricted searches for evidence of crime held by innocent third-parties who were engaged in First Amendment-protected activities. The PPA thus protects the confidentiality of non-evidentiary files held by this special group of innocent third-parties – such as drafts of articles not yet published and the research and other supporting information (e.g., notes and interviews) that are never intended to be published. To preserve the confidentiality of these designated materials, the PPA instructs investigators not to search for the evidence at all, but to compel the innocent third-parties to find and produce it themselves. Thus, subject to certain exceptions, the PPA generally limits searches for work-product and documentary materials held by third-parties who plan to use them to communicate to the public.

New issues arise with the PPA due to the exponential growth in computer use over the last decade. With the advent of the Internet and widespread computer use, almost any computer can be used to "publish" material. As a result, the PPA may now apply to almost any search of any computer. Because computers now commonly contain enormous data storage devices, wrongdoers can use them to store material for publication – material that the PPA protects – while simultaneously storing (in a commingled fashion) child pornography, stolen classified documents, or other contraband or evidence of crime.

4. Electronic Communications Privacy Act

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 et seq., in an effort to revise and expand the scope of the 1968 wiretap act. The statute attempted to strike a workable balance among the competing interests addressed in the statute at the time: the privacy interests of telecommunications users, the business interests of service providers, and the legitimate needs of government investigators.

Two factors have raised concerns about ECPA: (1) the statute treats wire and electronic communications inconsistently; and (2) use of the Internet has grown dramatically, and voice and non-voice data have converged. First, although ECPA attempted to create a technology-neutral framework for regulating the disclosure of electronic communications and records, it was only partially successful. For example, the 1986 legislation distinguished broadly between "wire communications" (such as voice telephone calls) and "electronic communications," which it accorded lesser protections. This inconsistency create practical problems in today's converged network environment where voice and non-voice data may be intertwined in a single data stream.

These inconsistencies take on additional significance with the now widespread use of computers and the Internet, because the proportion of criminal activity occurring online, or using telecommunications technologies, has increased over time. E-mail, voice mail, user access logs, and remotely stored files play an important, and in many cases, critical role in investigating and prosecuting crimes ranging from large-scale consumer fraud to extortion and murder.
These developments suggest that ECPA be carefully evaluated to ensure that it (1) takes into account new communications technologies in its treatment of wire and electronic communications; (2) has appropriate penalties for a variety of criminal invasions of communications privacy; (3) resolves deficiencies in the rules for government access to customer records, especially with respect to access by civil and regulatory agencies; and (4) cures omissions and inconsistencies within the statutory framework.

5. Telephone Harassment

The Internet and the widespread use of computers have created a host of new tools for communication. Existing statutes provide criminal penalties for persons who use telephones to harass or abuse others. For example, one provision of 47 U.S.C. § 223 makes it a federal crime, punishable by up to two years in prison, to use a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number. The statutory prohibition applies only if the perpetrator does not reveal his or her name. See 47 U.S.C. § 223(a)(1)(C).

The new means of communication by computer, however, have given computer users a new method of inflicting such abuse not covered by the existing laws. A malicious computer user, for example, can post an electronic message in which he pretends to be the person that he intends to harass (see cyberstalking box in Part II.A above). In this fraudulent message (that may reach thousands of people), he can state, for example, that he (posing as the victim) likes to participate in some particular sexual act and then invite anyone who reads the message to call the victim's home telephone number. Yet this form of harassment evades the prohibitions of 47 U.S.C. § 223, which applies only to direct

(1997)

To protect children from such risks, parents and teachers therefore need to empower themselves with the tools, knowledge, and resources to supervise and guide children's online experience and to teach children how to use the Internet responsibly.

1. Technological Tools

Technology provides tools that may assist in preventing children from accessing inappropriate materials on the Internet or divulging personal information about themselves or their families online. The most common technological tools are "blocking" and "filtering" software, as described more fully below.

(a) *Blocking Software*

"Blocking" software uses a "bad site" list and prevents access to those sites. The vendor of the software identifies specified categories of words or phrases that are deemed inappropriate and configures the blocking software to block sites on which the prohibited language appears. Although some vendors allow parents to customize the "bad site" list by allowing them to add or remove sites, others keep the list secret and do not permit parents to modify it.

Although such software can be a useful tool for restricting access to inappropriate websites in certain circumstances, they can also create a false sense of security, because they cannot restrict access to all inappropriate sites for children. The number of websites published each day far exceeds the ability of software companies to review the sites and categorize them for their "bad site" lists. 26 "Out of approximately 3 million separate websites in existence (each website may contain two or more separate webpages and the number of separate files, pages and graphics online is estimated at 330 million), only a small fraction have been reviewed, in aggregate, by child protection software companies." 27 Because the gap widens daily, with an estimated 160,000 new websites registered each month, "bad sites" will inevitably get through. 28

Another potential drawback is that most blocking software does not differentiate between the age of the users. What may be inappropriate for an eight year old, may be appropriate for a teenager. However, because most software only has one user setting to determine what should be blocked, either the teenager will be denied access to sites that are beneficial or the eight-year-old will be given access to sites that are inappropriate. In addition, in cases where software vendors do not allow parents to customize the "bad site" list, parents cannot make an informed decision on what material should be restricted. They must rely on the judgment of an unknown third party to decide what sites are acceptable for their children.

(b) *Filtering Software*

"Filtering" software blocks sites containing keywords, alone or in context with other keywords. For example, if parents wanted to restrict their child's access to sites related to drug use, the software would be configured to deny access to sites containing such

MLATs and domestic laws vary with regard to the requirements relating to a request for assistance. To issue subpoenas, interview witnesses, or produce documents, some MLATs and some laws permit assistance as long as the conduct under investigation is a crime in the requesting state, even where it is not also a crime in the requested state.

In the more sensitive area of searches and seizures, however, dual criminality (i.e., that the conduct under investigation is a crime in both the requesting and requested countries and is punishable by at least one year in prison) is often required (e.g., U.S./Netherlands MLAT). In other circumstances, a country can refuse a request if the request "relates to conduct in respect of which powers of search and seizure would not be exercisable in the territory of the Requested Party in similar circumstances" (e.g., U.S./U.K. MLAT). Finally, some MLATs and domestic laws permit assistance only if dual criminality exits and if the offense is extraditable (e.g., mutual assistance laws of Germany). With regard to extradition, the United States has entered into bilateral treaties with over 100 countries. These treaties are either "list treaties," containing a list of offenses for which extradition is available, or they require dual criminality and that the offense be punishable by a specified minimum period. Therefore, if one country does not criminalize computer misuse (or provide for sufficient punishment), extradition may be prohibited.

The issue of dual criminality is not an academic or theoretical matter. In 1992, for example, hackers from Switzerland attacked the San Diego Supercomputer Center. The U.S. sought help from the Swiss, but the investigation was stymied due to lack of dual criminality (i.e., the two nations did not have similar laws banning the conduct), which in turn impeded official cooperation. Before long, the hacking stopped, the trail went cold, and the case had to be closed.

The solution to the problems stemming from inadequate laws is simple to state, but not as easy to implement: countries need to reach a consensus as to which computer and technology-related activities should be criminalized, and then commit to taking appropriate domestic actions. Unfortunately, a true international "consensus" concerning the activities that universally should be criminalized is likely to take time to develop. Even after a consensus is reached, individual countries that lack appropriate legislation will each have to pass new laws, an often time-consuming and iterative process.

2. Multilateral Efforts

Although bilateral cooperation is important in pursuing investigations concerning unlawful conduct involving the use of the Internet, multilateral efforts are a more effective way to develop international policy and cooperation in this area. The reason for this stems from the nature of the Internet itself. Because Internet access is available in over 200 countries, and because criminals can route their communications through any of these countries, law enforcement challenges must be addressed on as broad a basis as possible, because law enforcement assistance may be required from any Internet-connected country. That is, even if two countries were able to resolve all the high-tech crime issues they faced, they would still (presumably) only be able to solve those crimes that involved their two countries. Multilateral fora allow many countries to seek solutions that will be compatible to the greatest extent with each country's domestic laws.

Several multilateral groups currently are addressing high-tech and computer-related

crime. Of these groups, the Council of Europe ("COE"), and the Group of Eight ("G-8") countries are the most active. To begin to address the need to harmonize countries' computer crime laws, the COE is drafting a Cybercrime Convention, which will define cybercrime offenses and address such topics as jurisdiction, international cooperation, and search and seizure. The Convention may be completed as soon as December 2000. After approval by a high-level committee, the Convention will be open for signature by COE members and non-member states which participated in the drafting. The G-8 Subgroup on High-tech Crime has been focusing on ways to enhance the abilities of law enforcement agencies to investigate and to prosecute computer- and Internet-facilitated crimes, such as establishing a global network of high-tech crime experts and developing capabilities to locate and identify those who use the Internet to commit crimes. In May 1998, President Clinton and his G-8 counterparts adopted a set of principles and an action plan, developed by the Subgroup, for fighting computer crime. The COE and G-8 efforts, as well as other international efforts, are described in more detail in Appendix J to this report.

3. Continuing Need for International Cooperation

As these multilateral efforts progress and as more formal mechanisms for cooperation are developed, law enforcement agencies in the U.S. and other countries are cooperating informally and have undertaken joint initiatives to achieve their goals. For example, the Customs Service has been involved in joint cyber-investigations with the German Federal police. These joint investigations have resulted in 24 referrals from Customs' Cybersmuggling Center to field offices during the last three months. In most instances, these referrals have led to the issuance of federal or state search warrants. Customs is also involved in joint efforts on Internet-related investigations involving money laundering and child pornography distribution with officials in countries such as Indonesia, Italy, Honduras, Thailand, and Russia.

As international issues become more prevalent in investigations of Internet-facilitated offenses, U.S. law enforcement agencies must continue to develop cooperative working relationships with their foreign counterparts. The 24/7 high-tech point-of-contact network established among the G-8 countries and others must continue to be developed and expanded to include more countries. In addition, the U.S. should continue to work with other countries, international groups, and industry to develop comprehensive and global plans for addressing the complex and challenging legal and policy issues surrounding jurisdiction raised by unlawful conduct on the Internet.

IV. THE ROLE OF PUBLIC EDUCATION AND EMPOWERMENT

The third component of the Working Group's 3-part strategy for responding to unlawful conduct involving the use of the Internet is to implement aggressive efforts to educate and empower the public to minimize risks associated with the Internet and to use the Internet responsibly through technological and non-technological tools. Although both types of tools can be extremely useful when used appropriately, "one size does not fit all." One must weigh the advantages and disadvantages in determining which set of tools will work best for an individual's particular situation.

This part of the report therefore discusses existing and potential new tools and resources

that can be used to educate and empower parents, teachers, and others to prevent or minimize the risks from unlawful conduct involving use of the Internet. First, we review the technological and non-technological tools that are available for parents and teachers to use to help ensure that children have a safe and rewarding experience online. Next, we discuss how consumers can educate themselves in order to avoid fraudulent and deceptive practices on the Internet. In particular, this part highlights how several federal agencies are using technology to educate consumers and how they are working with the private sector to develop effective consumer protection practices. Many other agencies are undertaking similar efforts. Last, we discuss government-industry cooperation efforts to educate the public on the importance of being good "cybercitizens."

A. Educating and Empowering Parents, Teachers, and Children

With the growing number of U.S. classrooms connected to the Internet and the rising number of personal computers used in the home, more and more children are now able to access the Internet. Almost 90 percent of public schools – including over 1 million classrooms – in the U.S. are connected to the Internet. Over 40 percent of American households own computers and one-quarter of all households have Internet access. 25

One of the greatest benefits of the Internet is the access it provides children to such things as educational materials, subject matter experts, online friendships, and penpals. Nevertheless, like many other pursuits that children engage in without adequate parental supervision, the Internet should also be approached with careful consideration of risks and benefits. One concern of course is that the Internet may allow children unrestricted access to inappropriate materials. Such materials may contain sexually explicit images or descriptions, advocate hate or bigotry, contain graphic violence, or promote drug use or other illegal activities. In the worst instances, children have become victims of physical molestation and harassment by providing personal information about themselves over the Internet and making contact with strangers.

"Although children can use the Internet to tap into the Library of Congress or download pictures from the surface of Mars, not all of the material on the Internet is appropriate for children. As a parent, you can guide and teach your child in a way that no one else can. You can make sure that your child's experience on the Internet is safe, educational, and enjoyable."

President Bill Clinton
A Message to Parents about the Internet, in The Parent's Guide to the Internet

words as "marijuana," "cocaine," "heroin," etc. Filtering software is available both directly and through some Internet service providers ("ISPs") such as Lycos or FamilyNet.

Filtering software can also be used to restrict access to inappropriate websites, but, like blocking software, they can be both underinclusive and overinclusive. They can, for example, filter sites that are either harmless or even desirable. With the example above, sites that promote drug rehabilitation, seeking help for a drug problem, or drug prevention would be blocked simply because they use the keywords. Another example of how filtering is over inclusive is denying access to the word "sex." While this filter would block certain sites with inappropriate sexual content, it would also block harmless sites that contained the words "sextuplets," "sexton," "Mars Exploration," among many others. In addition, some website operators have learned to bypass the filtering mechanism by misspelling the typical keywords. 29

Filtering software may also be used to block sites that have a particular label or rating. The content provider or a labeling service classifies the site in a particular category (e.g., "romance: no sex" or "explicit sexual activity") and the filtering software is programmed to deny access to sites with particular ratings. As with "bad sites," parents must rely on the judgment of unknown third parties to determine what is appropriate for their children. In this case, the content provider must self-label the site accurately or a labeling service must assign the appropriate label to the site. Another major drawback is that very few sites are labeled. Parents must decide whether to block or allow access to unrated sites. Blocking all unrated sites would deny access to harmless and educational material, while allowing access to all unrated sites would undoubtedly allow inappropriate material to get through.

(c) *Other Software*

Other types of software enable parents to monitor and control their children's use of the computer. For example, "monitoring and tracking" software allows parents to track how much time their children spend online, where their children go online, and how much time their children spend on the computer offline. "Outgoing filtering" software prevents children from sharing certain information with others over the Internet, such as their name, telephone number, and address. Every time the child tries to send the prohibited information to someone online, it shows up as "XXX."

2. Non-technological Tools

(a) *What Parents Can Do*

One of the most effective ways of protecting children from inappropriate material on the Internet is to teach them to use the Internet responsibly. Parents play a major role in this by taking responsibility for children's online computer use. By doing so, parents can greatly minimize any potential risks of being online.

There are certain safety tips parents can follow to ensure that their children use the Internet safely. These tips include:

words as "marijuana," "cocaine," "heroin," etc. Filtering software is available both directly and through some Internet service providers ("ISPs") such as Lycos or FamilyNet.

Filtering software can also be used to restrict access to inappropriate websites, but, like blocking software, they can be both underinclusive and overinclusive. They can, for example, filter sites that are either harmless or even desirable. With the example above, sites that promote drug rehabilitation, seeking help for a drug problem, or drug prevention would be blocked simply because they use the keywords. Another example of how filtering is over inclusive is denying access to the word "sex." While this filter would block certain sites with inappropriate sexual content, it would also block harmless sites that contained the words "sextuplets," "sexton," "Mars Exploration," among many others. In addition, some website operators have learned to bypass the filtering mechanism by misspelling the typical keywords. 29

Filtering software may also be used to block sites that have a particular label or rating. The content provider or a labeling service classifies the site in a particular category (e.g., "romance: no sex" or "explicit sexual activity") and the filtering software is programmed to deny access to sites with particular ratings. As with "bad sites," parents must rely on the judgment of unknown third parties to determine what is appropriate for their children. In this case, the content provider must self-label the site accurately or a labeling service must assign the appropriate label to the site. Another major drawback is that very few sites are labeled. Parents must decide whether to block or allow access to unrated sites. Blocking all unrated sites would deny access to harmless and educational material, while allowing access to all unrated sites would undoubtedly allow inappropriate material to get through.

(c) *Other Software*

Other types of software enable parents to monitor and control their children's use of the computer. For example, "monitoring and tracking" software allows parents to track how much time their children spend online, where their children go online, and how much time their children spend on the computer offline. "Outgoing filtering" software prevents children from sharing certain information with others over the Internet, such as their name, telephone number, and address. Every time the child tries to send the prohibited information to someone online, it shows up as "XXX."

2. Non-technological Tools

(a) *What Parents Can Do*

One of the most effective ways of protecting children from inappropriate material on the Internet is to teach them to use the Internet responsibly. Parents play a major role in this by taking responsibility for children's online computer use. By doing so, parents can greatly minimize any potential risks of being online.

There are certain safety tips parents can follow to ensure that their children use the Internet safely. These tips include:

• never give out personal information, such as home address, school name, or telephone number, in a public message such as a chat room or bulletin board;

• do not post photographs of children on websites or news groups that are available to the public;

• 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 place and be sure to accompany the child;

• never respond to messages that are suggestive, obscene, belligerent, threatening or make you feel uncomfortable;

• encourage children to tell you if they encounter such messages;

• report any inappropriate messages you receive immediately;

• consider keeping the computer in a room other than the child's bedroom to monitor his or her online use;

• get to know your children's online friends just as you get to know all of their other friends;

• set up specific rules for your children's online use, such as the time of day and length of time that they can be online and appropriate sites for them to visit. 30

There are many useful publications and websites for parents on this topic. For example, The Parent's Guide to the Internet (published by the U.S. Department of Education), Site Seeing on the Internet: A Guide to Traveling in Cyberspace (published by the FTC and the National Association of Attorneys General), and The Parent's Guide to the Internet: Raising Your Family on the Information Superhighway (by Travis West) explain the basics of the Internet, how it works, what is available online, and give guidance on how to ensure safe use of the Internet. For additional publications on responsible use of the Internet, visit www.childrenspartnership.org for a list of resources.

Likewise, there are many websites that give parents guidelines to promote safe, rewarding online experiences for children. For example:

• www.getnetwise.org – This website was created by 15 Internet companies as a comprehensive resource guide for parents. It includes instant access to tools representing the latest technologies that allow parents to block and filter inappropriate content, monitor the websites and chat rooms that their children visit, and set strict time limits on their children's online sessions. It also includes access to information on how to report a crime or other troubling activity online and provides a guide to quality, educational websites

beneficial to children. The website also provides safety tips for online use.

• www.americalinksup.org – This website seeks to bring the online industry, families, teachers, librarians and other children's advocates together to ensure that children have a rewarding and educational online experience. It provides safety tips for parents and children; access to discussion groups of parents, teachers and other Internet users on critical safety issues; links to more than 700 quality websites for children reviewed and recommended by children's librarians; and information on local events where parents and children can learn about Internet basics and tools that promote rewarding online experiences.

• www.cyberangels.org – This website has been in existence since 1995 and is considered the largest Internet safety and education program. In addition to providing parents guidance on how to supervise their children online, it teaches children how to use the Internet safely with material geared toward them. For example, children can join Sophia's Safe Surfing Club, take a safe surfing quiz, and earn a safe surfing permit. Cyberangels also has Net Patrol teams that regularly monitor the Internet for child-crimes, cyberstalkers, and fraudulent scams and report it to law enforcement authorities. The website provides support groups for victims of stalking and harassment over the Internet and gives tips on how to document and report cyber-stalking. CyberAngels also provides links to safe sites and reviews and recommends blocking/filtering software.

• www.parentech.org – This site provides families and educators of middle school children (grades 6-8) with free resources focusing on how technology affects education, careers, and society. It includes parent and teacher guides in these three areas. For example, the parent's guide on technology and education has articles on how to help middle schoolers get the most out of learning with technology, a parent's guide to classroom technologies, and technology standards for middle schools. The teacher's guide to technology and careers includes articles on what skills are necessary for these careers and how to develop those skills at the middle school level. In addition, the site has a discussion corner where parents and educators can share ideas, concerns, and questions with each other and with experts from across the nation.

• www.safekids.com – This website contains various articles about Internet basics and online safety, guidelines for parents on how to supervise their children on the Internet, safety tips for children, and filtering/blocking software reviews. In addition, the site has links to other sites that offer Internet advice to parents and includes a link to report online crime against children.

(b) *What Schools and Libraries Can Do*

As increasing numbers of children have access to the Internet from their schools and neighborhood libraries, we need to address the issue of how best to ensure that these

children have positive, age-appropriate, educational online experiences. The Administration has taken the view that empowering parents, teachers, and librarians with a wide range of tools with which they can protect children in their community in a manner consistent with their values is ultimately the most effective approach and one that is most compatible with the First Amendment. 31

Schools and libraries are currently using a wide range of technology tools and monitoring techniques to ensure that children do not encounter inappropriate material or dangerous situations while online. These schools and libraries are determining what will work best in their particular schools and communities. Absent proof that local decision making is not working to protect our children, the federal government should not mandate a particular type of technology, such as filtering or blocking software. Rather, we should encourage "acceptable use" policies ("AUPs") by all public institutions that offer access to online resources, including the Internet. Such policies may include the use of blocking and filtering technologies, or they may involve the use of monitoring, smart cards, or codes of conduct. An AUP should, while being sensitive to local needs and concerns, offer reasonable assurances to parents that safeguards will be in place in the particular school or library setting that permit users to be empowered to have educational experiences consistent with their values.

In addition to AUPs, schools may also use "intranets" to restrict student access to inappropriate material. An intranet is a controlled computer network that uses similar software and transmission mechanisms as the Internet, but is accessible only to those who have permission to use it (an intranet is generally confined to users within an organization). These controls permit the intranet system managers to limit user access to Internet material as well as to restrict those outside the network from being able to reach it.

Schools and districts may also use Regional Technology and Education Consortia organizations ("RTECs") as a resource. Six regional consortia, funded by the Department of Education, assist and support states, districts, schools, and other educational institutions in the use of advanced technologies to improve teaching and student achievement. In helping schools and districts with planning and implementation of technology, RTECs can help schools identify Internet safety solutions that meet the schools' needs and policy preferences. In addition, RTECs also provide resources for teacher training in technology.

(c) *Next Steps*

The Department of Justice and the Department of Education have funded a study by the National Academy of Sciences on how to protect children from inappropriate material on the Internet. This study will include a description of the risks and benefits of various tools and strategies that can be used to protect children from inappropriate material, an analysis of how the different tools and strategies can be used together, and case studies of how different communities have approached this problem. The final report is scheduled to be completed in November 2001.

In addition, in October 1998, Congress passed the Child Online Protection Act ("COPA") 32 that, among other things, established a Commission on Online Child

Protection to examine the extent to which current technological tools effectively help protect children from inappropriate online content. The members of the commission were appointed last year, with the final members coming on board in October 1999, and the commission's report is due to Congress in November 2000.

Finally, the Departments of Commerce, Education, and Justice are planing a joint effort to host a roundtable discussion with industry representatives, especially those in the software industry, to discuss the benefits and limitations of existing blocking and filtering software. These discussions can lay the groundwork for future software contributions to Internet safety.

B. Educating and Empowering Consumers

The electronic marketplace offers consumers unprecedented choice and around-the-clock accessibility and convenience. It gives established marketers and new entrepreneurs low-cost access to a virtually unlimited customer base. With these benefits, however, comes the challenge of ensuring that the virtual marketplace is a safe and secure place to purchase goods, services, and digitized information. Consumers must be confident that the goods and services offered online are fairly represented and the merchants with whom they are dealing -- many of whom may be located in another part of the world -- deliver their goods in a timely manner and are not engaged in illegal business practices like fraud or deception. Consumer confidence also requires that consumers have access to fair and effective redress if they are not satisfied with some aspect of the transaction.

This section highlights some of the Federal Trade Commission's initiatives to educate consumers through technology; the Department of Commerce's coordination efforts with the private sector to develop effective consumer protection practices; and the Food and Drug Administration's outreach campaign regarding medical products on the Internet. As described more fully below, the FTC has made innovative use of the Internet to educate and alert consumers about fraud and deceptive practices online, to disseminate its publications, to investigate potential violations, and to receive and respond to consumer complaints. The Department of Commerce has also worked with consumer and business representatives to develop codes of conduct for electronic commerce and mechanisms for consumer dispute resolution, redress, and enforcement. In addition, the FDA has used the Internet to educate consumers and health professionals about the possible risks of ordering prescription medications and other medical products on the Internet, and the Securities and Exchange Commission ("SEC") has likewise used the Internet to help investors avoid online securities fraud. The Postal Inspection Service posts consumer fraud prevention "tip sheets" and other fraud prevention information on its website (www.usps.gov/postalinspectors). And, as part of its Internet Fraud Initiative, the Department of Justice has been active in public education and outreach efforts to prevent online fraud (e.g., establishing a website on identity theft and fraud (www.usdoj.gov/criminal/fraud/idtheft)), and the FBI has prepared an online Parent's Guide to Internet Safety (www.fbi.gov).

1. FTC Initiatives: Using Technology to Educate Consumers

The FTC is committed to stemming fraudulent, misleading, and deceptive trade practices through actions that involve both law enforcement and education. Acting on the belief

that the most effective consumer protection is education, the FTC has sought to help alert as many consumers as possible to the telltale signs of fraud, the importance of privacy in the information age, and other critical consumer protection issues. Use of the Internet to develop and disseminate information about fraud and technology-related matters is integral to the FTC's education, deterrence, and enforcement efforts and has allowed the agency to reach vast numbers of consumers and businesses quickly, simply, and at low cost.

(a) *Fraud Prevention Information for Consumers*

More than 200 of the consumer and business publications produced by the FTC's Bureau of Consumer Protection are available on the agency's website in text and .pdf format. Indeed, the difference in the number of publications viewed online in 1996 and 1999 (140,000 versus 2.5 million page-views) tells the story of the Internet's coming of age as a mainstream medium and its importance to any large-scale dissemination effort. Those 2.5 million page views are in addition to the 6 million print publications distributed each year to organizations that disseminate them on the FTC's behalf.

(b) *Link Program*

The FTC also actively encourages "partners" – government agencies, associations, organizations, and corporations with an interest in a particular subject – to link to the FTC's website from their sites and to place banner public service announcements provided by the FTC on their sites. Links from the banners allow visitors to click through to the FTC site quickly to get the information the user is looking for exactly when they want it. Among the organizations that have helped drive traffic to the consumer information on www.ftc.gov are the Alliance for Investor Education, the Arthritis Foundation, the American Association of Retired Persons, American Express, the Better Business Bureau, CBS, Circuit City, motleyfool.com, the National Institutes of Health, the North American Securities Administrators Association, Shape Up America!, the U.S. Patent and Trademark Office, and Yahoo!.

(c) *"Sting" Pages*

Many Internet shoppers looking for weight loss products will find an attractive-looking site that trumpets NordiCaLite, a "safe and natural" way to lose weight. Three clicks into the sales pitch, the FTC seal appears, alerting consumers that the site was put up by the federal agency, that the product is a fake, and that certain words and phrases are tip offs to help them avoid most rip offs.

Too often, warning information about frauds reaches consumers after they've been scammed. For the FTC, the challenge is how to reach consumers before they fall victim to a fraudulent scheme. Knowing that many consumers use the Internet to shop for information, agency staff develop "sting" sites that mimic the characteristics of a site selling fraudulent products or services. "Metatags" embedded in the FTC websites make them accessible to consumers who are using major search engines and indexing services as they look for products, services, and business opportunities. The "sting" websites link back to the FTC's webpage, where consumers can find the practical, plain English information they need. The agency has developed 13 "sting" sites on topics ranging from

health care products to scholarship services to vacation deals and investments, and feedback from the public has been overwhelmingly positive. Many visitors express appreciation -- not only for the information, but also for the novel, trouble-free, and anonymous way it is offered.

(d) *Tutorials*

The FTC has also developed interactive puzzles and games to reinforce the concepts spelled out in its brochures, 1-page "news you can use" consumer alerts, and graphics. For example, to mark the first anniversary of the Telemarketing Sales Rule in December 1996, the FTC placed a recording of a fraudulent telemarketing call on its website and developed a quiz to test a consumer's ability to tell the difference between a legitimate call and fraudulent one. Later, the Field of Schemes investment fraud initiative included the launch of an online quiz called "Test Your Investment I.Q." A series of typical telephone misrepresentations asked consumers to define an investment offering as solid or risky and then explained the answers. As part of Project Mousetrap, which dealt with fraudulent invention promotion firms, the FTC created an activity designed to test a reader's "patent-ability": a crossword puzzle containing critical terms from the world of patents and idea promotion. And to support the first National Consumer Protection Week, an online crossword puzzle, a true-false quiz, and a word find that focused on credit terms were developed for the National Consumer Protection Weekly, a newsletter that was distributed electronically to consumer agencies, law enforcement officials, and corporations across the country.

(e) *Consumer.gov*

Armed with a vision of the Internet as a powerful tool for consumer education and empowerment, the FTC convened a group of five small federal agencies in 1997 to develop and launch a website that would offer 1-stop access to the array of federal consumer information. On the theory that consumers may not know one federal agency from another, the information is arranged topically. Federal agencies and consumers have responded well to www.consumer.gov. The site includes contributions from over 100 federal agencies and logs some 79,000 user sessions a month, each of which last an average of over four minutes. The site also houses special initiatives: The President's Council on Y2K Conversion asked the FTC to establish a Y2K consumer information site; the Quality Interagency Coordination Task Force requested a special site on health care quality; and the U.S. Postal Inspection Service asked that www.consumer.gov house the site to support the "kNOw Fraud" initiative, a public-private campaign that involved sending postcards about telemarketing fraud to 115 million American households in the fall of 1999. The original www.consumer.gov team received the Hammer Award for its efforts. The FTC continues to maintain the site.

(f) *Spam Mailbox*

Millions of consumers are besieged by unsolicited commercial e-mail ("UCE") or "spam" every time they open their e-mailboxes. At best, spam is annoying. At worst, it is costly and disruptive to consumers. 33 Hoping to relieve consumer frustration and gain a foothold on deceptive e-mail offers, the FTC invited consumers to forward their spam to a special address (uce@ftc.gov). With 3,000 e-mails arriving each day, the FTC has been

able to build a spam database that is an extremely helpful resource for investigators. With partners from the Postal Inspection Service, the agency lets "junk e-mailers" know how not to break the law, and lets consumers know how to recognize the 12 most common types of e-mail fraud, known as the "dirty dozen."

(g) *Online Complaint Handling*

By 1998, with consumer use of the Internet to access information, entertainment, products and services becoming routine, the FTC began accepting consumer complaints electronically. The consumer response to the online complaint feature indicates that the FTC is meeting a real need: The agency receives online – and responds online to – an estimated 1,000 complaints and inquiries a week.

(h) *Business Education for Online Marketers*

As part of its mission, the FTC provides guidance to online marketers on how to assure that basic consumer protection principles apply online. Many of these entrepreneurs, new to the Internet and to marketing in general, may be unfamiliar with consumer protection laws. But even experienced marketers have raised novel issues in their efforts to apply traditional consumer protection laws to the online environment. The FTC has used a variety of approaches to get its consumer protection messages out to the business community, from compliance guides, brochures and speeches at industry and academic meetings and conferences to e-mails and Web-based public service announcements, staff advisory letters on www.ftc.gov, use of the trade press to promote the availability of information on the agency site, and workshops on issues of interest and posting the transcripts.

(i) *Publications for Business*

Among the publications for business that have been distributed widely in print and online are Advertising and Marketing on the Internet: Rules of the Road, which has had a print distribution of over 22,000 and over 33,000 page-views of the online version. In addition, two business alerts – Selling on the Internet: Prompt Delivery Rules and Website Woes: Avoiding Web Service Scams – have been widely disseminated.

(j) *Surfs*

Just as consumers were discovering the benefits of "surfing" the Internet for instant access to information, FTC staff saw the value of surfing to educate businesses and to investigate potential legal violations. Since December 1996, when the FTC organized its first "surf" to ferret out pyramid schemes, it has become clear that this tool gives new meaning to efficiency. To date, the FTC has led some 20 surfs, with over 250 agencies and consumer protection agencies around the world, identifying some 4,000 commercial websites that make dubious claims, largely in the promotion of health and diet products, pyramid schemes, business opportunities, investments, and credit repair.

Internet surfs allow law enforcement officials to survey the nature and scope of particular violations online. They also offer an opportunity to educate website operators – many of whom are new entrepreneurs unaware of existing laws – instantly and directly. When

agency staff surfers identify a site that may have problems, they send an e-mail message that explains why the site may violate the law. Their message also provides a link to the FTC website for more information and gives notice about a follow-up visit. These follow-up surfs reveal that about 20 to 70 percent of the problem sites in a particular area are improved or removed. Those sites that continue their problem practices may be subject to further investigation and enforcement.

(k) *Protecting Privacy Online*

In May 1998, at the request of the Vice President, the FTC used www.consumer.gov to unveil a 1-stop shop for information about how to protect one's privacy both on and off the Internet. The "About Privacy" site explains consumer privacy rights and provides visitors with contact information to ask that their personal information not be shared with third parties. For example, the page provides information on how to contact credit bureaus, state motor vehicle offices, and marketing organizations via the web, telephone, or mail. It includes sample opt-out letters that consumers can tailor to their own needs, as well as hyper-links to each of the three major credit reporting bureaus and the Direct Marketing Association's opt-out pages.

In addition, the FTC has initiated a major multi-pronged information campaign focused on the provisions of the recent Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506, which requires parental permission before collecting data from those under 13 years old. See Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312 (1999). Businesses are being alerted to their responsibilities, and parents and youngsters are learning about their rights under the law.

2. Department of Commerce Initiatives

U.S. government policymakers and law enforcement officials are working to ensure consumer confidence in the virtual marketplace by enforcing existing legal protections and encouraging private sector leadership. Last spring, the Department of Commerce challenged the private sector to work with consumer representatives to develop effective consumer protection practices, including developing codes of conduct for business-to-consumer electronic commerce and alternative, easy-to-use mechanisms for consumer dispute resolution, redress, and enforcement. This approach recognizes that as e-commerce expands to encompass more international business-to-consumer transactions, alternative, easy-to-use mechanisms for consumer dispute resolution, redress and enforcement can help to ensure strong and effective consumer protection in the online environment and obviate the need for immediate resolution of the difficult issues surrounding jurisdiction and choice of law that would result if disputes had to be resolved in the courts.

There have been several significant responses to this challenge. In June 1999, the Better Business Bureau's online division, BBBOnLine, announced a project to develop a Code of OnLine Business Practices (see www.bbbonline.org). BBBOnLine will work with industry, consumer representatives and government to develop a code to provide online merchants with guidelines to implement important consumer protections, such as disclosure of sale terms, data privacy, dispute resolution mechanisms, and non-deceptive advertising.

A similar effort was initiated in August 1999 with the formation of the Electronic Commerce and Consumer Protection Group, whose members include a number of industry leaders such as America Online, American Express, AT&T, Dell, IBM, Microsoft, Time Warner Inc., and Visa. This group is committed to working with consumer leaders to address electronic commerce confidence issues by formulating concrete approaches to protect consumers and facilitate e-commerce (see www.ecommercegroup.org).

3. FDA's Outreach Campaign

As part of a major public education campaign, the FDA is informing consumers about the potential public health risks of buying medical products on the Internet. To increase awareness, FDA has developed a multimedia education campaign that includes messages targeted to specific audiences and the formation of partnerships for creating and disseminating information through government agencies, national organizations, consumer groups, and the Internet industry. The campaign will include public service announcements, brochures, newspaper articles, media interviews, and an FDA website (www.fda.gov).

FDA's website on buying medical products online provides information on how consumers can protect themselves from certain online practices involving the sale of FDA-regulated products; reports on FDA's enforcement efforts; advice on spotting health care fraud; and answers to frequently asked questions about online drug sales. Consumers who suspect that a website is illegally selling human or animal drugs, medical devices, biological products, foods, dietary supplements, or cosmetics can also complete and submit to FDA an electronic complaint form provided at the site.

4. SEC's Investor Education Efforts

The Securities and Exchange Commission ("SEC") believes that an educated investor is the best defense – and offense – against securities fraud. Investors who know what questions to ask and how to detect fraud will be less likely to fall prey to con-artists, on or off the Internet. And, because they are more likely to report wrongdoing to the SEC and their state securities regulators, educated investors serve as an important early warning system to help regulators fight fraud. In particular, the SEC's Internet mailbox (help@sec.gov) and online complaint form have made it easy and convenient for investors to express concerns and to report complaints to the agency.

The SEC publishes and distributes more than a dozen free brochures that explain in plain English how the securities industry works, how to invest wisely, and what to do if something goes wrong. They include Internet Fraud: How to Avoid Online Investment Scams, which helps investors identify different types of Internet fraud, describes what the SEC is doing to fight Internet investment scams, and explains how to use the Internet to invest wisely. These and other materials are available on the SEC's website (www.sec.gov/consumer/online.htm).

Because investors increasingly use the Internet to research investment opportunities and to buy and sell securities, the SEC in 1999 launched a revised investor education page on

the SEC's website (www.sec.gov/invkhome.htm). The new page features interactive quizzes and calculators, information about online investing, tips for avoiding Internet fraud, and a special section for students and teachers. The page also features the SEC's latest investor alerts, such as Tips for Online Investing: What You Need to Know About Trading in Fast-Moving Markets and Day Trading: Your Dollars at Risk. In addition to individual securities firms, a number of financial services industry associations, educational organizations, consumer groups, media outlets, and publicly traded companies provide links from their websites to the SEC's website.

5. CPSC's Consumer Outreach Efforts

An important part of the mission of the Consumer Product Safety Commission ("CPSC") is to inform and to communicate with the public about consumer product safety issues. Because banned or recalled products can find their way into commerce via the Internet, it is important for consumers to have direct access to safety information. Through its web site (www.cpsc.gov), the CPSC educates the public about critical product safety issues; provides a secure and efficient means by which consumers can report unsafe products; and provides a medium through which manufacturers, importers and distributors of consumer products can report substantial hazards associated with their products.

C. Developing Cybercitizens

Children and young adults are the fastest growing group using the Internet. Helping children draw conclusions about behavior and its consequences in cyberspace is an important part of educating responsible (future) online users. Although most children are taught at an early age that it is wrong to break into a neighbor's house or read their best friend's diaries, we must also emphasize that it is equally wrong, and potentially more damaging, to break into their neighbor's computers and snoop through their computer files. Computer hacking "for fun" is a very serious problem, not only for the targets of the attacks, but also for law enforcement personnel who often have no way to determine the motivation for and the identity of the person behind the intrusion.

Educating children (and adults) about acceptable online behavior is crucial for the Internet to continue to grow as a safe and useful medium. Likewise, there is a need to educate the public on the dangers posed by cybercrimes and how harm can be reduced if people use technology responsibly. As the proliferation of low-cost computers and networks has spread information technology to every corner of society, people of all ages who use this technology must understand that along with the obvious benefits of technology comes a set of corresponding responsibilities. To this end, the Attorney General announced in April 1999 that the Department of Justice had joined with the Information Technology Association of America ("ITAA") for a partnership on a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens.

The Cybercitizen Awareness Program seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children:

- An understanding of cyberspace benefits and responsibilities;
- An awareness of potential negative consequences resulting from the misuse of the medium;
- An understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed; and
- An ability to commit to adhere to these principles as they mature.

Thus far, the campaign has received $300,000 in grants from the Department of Justice's Office of Justice Programs. The partnership awarded a contract to a public relations firm in December 1999 to implement the objectives of the campaign. The Department of Justice and ITAA believe that the program will play a significant role in deterring potential hacking, educating the public about the potential dangers of the Internet, raising awareness about the potential consequences of online activities, reducing the threat to the nation's critical infrastructure, increasing online security in the United States, and providing savings to information technology resources owners and users who suffer economic losses as a result of computer crimes.

In addition to the awareness program detailed above, the Cybercitizen Partnership also has initiated a personnel exchange program between private business and federal agencies that is designed to educate both groups about how the other responds to threats and crimes over the Internet. This initiative will allow companies to find out how best to help law-enforcement agencies, and government officials will learn what business interests and influences drive industry decisions. The exchange program will be coordinated by the ITAA, which intends to detail personnel from the private sector to the FBI's National Infrastructure Protection Center. The partnership also expects to create a directory of computer experts and computer security resources so that law enforcement will know where to turn when they need assistance from industry.

V. CONCLUSIONS AND RECOMMENDATIONS

Ensuring the safety and security of those who use the Internet is a critical element of the Administration's overall policy regarding the Internet and electronic commerce, a policy that seeks to promote private sector leadership, technology-neutral laws and regulation, and an appreciation of the Internet as an important medium for commerce and communication both domestically and internationally

Consistent with the Administration's overall policy, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- First, any regulation of unlawful conduct involving the use of the Internet should be analyzed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner, and in a manner that accounts for other important societal interests such as privacy and protection of civil liberties;

• Second, law enforcement needs and challenges posed by the Internet should be recognized as significant, particularly in the areas of resources, training, and the need for new investigative tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and

• Third, there should be continued support for private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users to prevent and minimize the risks of unlawful activity.

The challenges to the federal government of unlawful conduct involving the use of the Internet are many. On one hand, the Internet offers unparalleled opportunities for socially beneficial endeavors. At the same time, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, and the unlawful distribution of computer software or other creative material protected by intellectual property rights.

In its analysis of existing federal laws, the Working Group finds that existing substantive federal laws generally do not distinguish between unlawful conduct committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication. To the extent these existing laws adequately address unlawful conduct in the offline world, they should, for the most part, adequately cover unlawful conduct on the Internet. There may be a few instances, however, where relevant federal laws need to be amended to better reflect the realities of new technologies, such as the Internet.

Despite the general adequacy of laws that define the substance of criminal and other offenses, however, the Working Group finds that the Internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include the need for real-time tracing of Internet communications across traditional jurisdictional boundaries, both domestically and internationally; the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for hand-in-glove coordination among various law enforcement agencies; and the need for trained and well-equipped personnel – at federal, state, local, and international levels – to gather evidence, investigate, and prosecute these cases. In some instances, federal procedural and evidentiary laws may need to be amended to better enable law enforcement to meet these challenges.

Indeed, the Working Group concludes that the federal government must continue to devote further attention to these important challenges. The report contains specific suggestions on areas on which additional resources and further evaluation are needed. These recommendations recognize that there are no easy answers to the challenges posed by unlawful conduct on the Internet. At the very least, however, significant attention should be given to the issues, and open dialogue and partnerships among law enforcement

agencies, industry, and the public must continue.

In light of its mandate, the Working Group confined its analysis to existing federal laws. A logical next step would be an expanded analysis of state (and, to the extent relevant, local) laws that focuses on whether those laws are adequate to investigate and prosecute unlawful conduct on the Internet. Because coordination and cooperation among federal, state, and local law enforcement agencies are key to our efforts to prevent, deter, investigate, and prosecute such unlawful conduct, such an analysis would provide states and others with a blueprint for translating the conclusions in this report into a more comprehensive approach to meeting the substantial challenges presented.

Finally, an essential component of the Working Group's strategy is continued support for private sector leadership, industry self-regulation, and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users so as to prevent and minimize the risks of unlawful activity. This Administration has already initiated numerous efforts to educate consumers, parents, teachers, and children about ways to ensure safe and enjoyable Internet experiences, and those efforts should continue. The private sector has also undertaken substantial self-regulatory efforts – such as voluntary codes of conduct and appropriate cooperation with law enforcement – that show responsible leadership in preventing and minimizing the risks of unlawful conduct on the Internet. Those efforts must also continue to grow. Working together, we can ensure that the Internet and its benefits will continue to grow and flourish in the years and decades to come.

---

1 See Towards Digital eQuality (1999) (Second Annual Report of the U.S. Government Working Group on Electronic Commerce) <http://www.ecommerce.gov/annrpt.htm>; A Framework for Global Economic Commerce (1997) <http://www.ecommerce.gov/framework.htm>.

2 The "Internet" has been defined as "collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio." Internet Tax Freedom Act, Pub. L. No. 105-277, Div. C, tit. 11, § 1101(e)(3)(C); Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, Div. C, tit. 13, § 1302(6). Internet connections are made using the same kinds of lines, cables, and satellites as those that join telephones. Unlike traditional telephone calls, however, which transmit information by circuit-switching (i.e., the use of a dedicated circuit between a caller and a call recipient, much like the string between two cans), the Internet transmits information by packet-switching. In packet-switching, communications are broken into small pieces, and each piece is placed into a packet. Each packet is sent individually to the recipient, with packets arriving at their destination through different routes. The communication is then reconstructed at the receiver's end.

3 Internet Users Now Exceed 100 Million, N.Y. Times, Nov. 12, 1999, at C8.

4 Forrester Research, U.S. Online Business Trade will Soar to $1.3 Trillion by 2003 (visited Dec. 17, 1998) <http://www.forrester.com>.

5 Cf. 1999 CSI/FBI Computer Crime and Security Survey, 5 Comp. Security Iss. & Trends 1 (Winter 1999) (discussing results of voluntary, anonymous survey of computer security breaches and noting uncertainties). Truly reliable estimates of computer crime are not currently available, because (1) there is no commonly accepted definition of a computer crime; thus, it is unclear whether certain criminal

activity should be included, or excluded, from computer crime statistics; (2) for a variety of reasons discussed in this report, most computer crimes are still not detected or reported; and (3) even when such crimes are reported, they are not reported to any central authority for compilation.

6 For example, in November 1999, an Internet bookseller, which also operated an Internet communications service that provided e-mail service to its book-dealer customers, was charged with intercepting its customers' electronic communications and possessing, without authorization, customer password files with intent to defraud. During a 6-month period in 1998, the bookseller was alleged to have intercepted e-mail messages from its dealers to Amazon.com in an attempt to gain a competitive commercial advantage for its own book-selling business by compiling a database of dealer purchases and by gathering information to analyze the book-selling market. The bookseller intercepted and copied thousands of e-mail communications to which it was not a party and was not entitled. As a result of this prosecution, the bookseller agreed to pay a $250,000 fine as part of a plea agreement.

7 In addition, safety nets created by existing regulatory systems to protect consumers from unlawful conduct in the offline world should be examined for their ability to protect consumers from unlawful conduct in the online world.

8 "Cross-site scripting" is a serious problem that hides computer code in links to popular Internet sites and is not limited to software created by a particular company or a particular web browser. Private sector cooperation and awareness are vital to protecting consumers against this potential exploit. Recognizing this, many private-sector leaders are educating consumers and Internet businesses about the "cross-site scripting" problem. Indeed, several computer companies published information on their websites regarding the exploit and its hazards within a day after the warning was issued.

9 For example, though beyond the scope of this report, the increasingly global nature of e-commerce can raise law enforcement issues in the areas of tax evasion, see 26 U.S.C. § 7201; tax fraud, see id. § 7206 (1); and money laundering, see 18 U.S.C. § 1956. The use of offshore foreign trusts and the ability to move assets electronically and to conduct financial transactions over the Internet can place information beyond the reach of criminal investigators. Emerging technologies, such as cyberbanking, stored value cards, and Internet brokerages can also be used to facilitate the hiding of assets from U.S. taxing authorities or placing them beyond their reach.

10 The distribution of hate speech, for example, raises particularly difficult policy questions. Germany, in light of its history, prohibits neo-Nazi speech and the distribution of hate literature. But Germans and others now complain not only that neo-Nazi speech itself is suddenly accessible throughout German via the Internet, but also that hate literature and similar materials are sent or made available via the Internet to customers in Germany from other countries, including from U.S.-based websites.

11 Technological solutions will, of course, play an important role in how the issue of online identification evolves and is resolved. Industry continues to develop new technological methods for verifying the identity of individuals, such as digital signature protocols and biometric technologies, but the full range of these technologies has not yet been fully perfected. As these new technologies emerge and grow, they should be evaluated for their benefits, as well as their limitations, for law enforcement and online commerce.

12 For further discussion of the availability of bombmaking information on and off the Internet, see U.S. Dep't of Justice, Report on the Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Existing Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent with the First Amendment to the United States Constitution (1997) (report submitted to the U.S. House of Representatives and the U.S. Senate pursuant to section 709(a) of the Antiterrorism and Effective Death Penalty Act of 1996) <www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html>.

13 Coordination among law enforcement, intelligence, and defense agencies is particularly important, because the origin and motive of a cyberattack can be difficult to ascertain, at least at the outset of an

attack. The government agency with responsibility for responding to a cyberattack, and the nature of the response, is likely to turn on the particular circumstances of the attack.

14 These efforts may include, for instance, technological solutions, information-sharing arrangements, appropriate monitoring or other system security mechanisms, the timely reporting of potential intrusions or other cybercrimes, and educational and other outreach efforts.

15 Russian KGB agents were apparently paying the hacker, sometimes using cocaine as currency, to gather information on the United States's "star wars" missile defense program. Stoll's 10-month odyssey in search of the hacker is recounted in his book, The Cuckoo's Egg: Tracking A Spy Through The Maze of Computer Espionage (1989).

16 See Remarks of the Honorable Janet Reno, Attorney General of the United States, to the National Association of Attorneys General (Jan. 10, 2000) <www.usdoj.gov/ag/speeches/2000/011000naagfinalspeech.htm>.

17 An example of an industry practice that leaves carriers without critical data is the generation and maintenance of records for local telephone calls. In the past, most Americans received an itemized list of all of their local telephone calls (i.e., calls within their area code or state) with their monthly telephone bill. But as telephone companies moved to bulk or flat-rate billing for local calls, there was no longer a revenue-based reason to list this information in phone bills and, indeed, to collect the information at all. As a result, when law enforcement needs records to confirm that a suspect dialed an ISP from his or her home (a local telephone call), that information will not exist if it was never collected in the first place.

18 Some countries require by law that data routinely be retained, while other countries explicitly prohibit such retention. A third sub-set of countries leave it to the marketplace to determine what should be retained.

19 See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. 31 (L 281); Directive 97/66/EC of the European Parliament and of the Council of December 15, 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, O.J. 1 (L 24) (Jan. 30, 1998). See generally Peter Swire & Robert Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (1998).

20 Because advertising revenue for a website is often tied to the level of visitor traffic, website operators often offer free e-mail accounts as a way of increasing their customer base.

21 Gary H. Anthes, "Stealth E-mail" Poses Corporate Security Risk, Computer World, Feb.12, 1996, at 1A (available at 1996 WL 2371156).

22 For example, an unsophisticated computer user may believe that he has deleted files containing child pornography when, in fact, that evidence is still on the computer and can be retrieved by a computer forensics expert. At the same time, however, a sophisticated computer user could "hide" evidence on a computer that is inaccessible to a law enforcement forensics expert. There have also been cases where computer users have "booby-trapped" evidence on a computer so that if a particular file is accessed, it is destroyed or made incomprehensible.

23 The San Diego Regional Computer Forensics Laboratory, which provides computer forensic analysis and support to the law enforcement community in Southern California, is a joint project among 32 federal, state, and local law enforcement agencies. It is staffed by 16 computer forensic examiners and a lab director. All of the personnel are detailed from their parent agencies and departments, most on a full-time basis. They represent five federal agencies and seven non-federal police agencies. Thirteen of the 15 staff members (11 non-FBI) have been trained by the FBI's Computer Analysis and Response Team

("CART"). The remaining three have received substantial training through their agencies. The lab has received substantial financial support from the California Border Alliance Group and has been provided space and resources by the FBI. More information about the lab can be found at http://www.usdoj.gov/usao/cas/sdlab.htm.

24 See generally U.S. Dep't of Justice, The National Information Infrastructure Protection Act of 1996: A Legislative Analysis (1996) <http://www.usdoj.gov/criminal/cybercrime/ 1030_anal.html>.

25 See U.S. Dep't of Commerce, Falling Through the Net: Defining the Digital Divide (July 1999).

26 Parry Aftab, Parents' Guide to the Internet: And How to Protect Your Children in Cyberspace (1998).

27 *Id.*

28 *Id.*

29 *Id.*

30 Lawrence J. Magid, Child Safety on the Information Highway (1998) <http://www.safekids.com/child_safety>.

31 See Letter from Assistant Secretary of Commerce Larry Irving to Federal Communications Commission Chairman William E. Kennard (Apr. 7, 1999) (encouraging acceptable use policies for public institutions offering access to the Internet).

32 COPA restricts the dissemination of "obscene" materials and materials "harmful to minors" over the world wide web. See 47 U.S.C. § 231. The statute provides an affirmative defense to liability, however, if the website attempts to screen minors from viewing the materials by requiring access through a credit card, debit card, or adult identification number. See id. § 231(c). COPA's restriction on communications that are "harmful to minors" has been challenged by various commercial entities and civil liberties groups on First and Fifth Amendment grounds, and a district court has entered a preliminary injunction as to its enforcement with respect to such communications. See ACLU v. Reno, 31 F. Supp. 2d 473 (E.D. Pa. 1999), appeal pending, No. 99-1324 (3d Cir. argued Nov. 4, 1999).

33 Several bills were introduced in the most recent session of Congress to regulate and limit spam. For instance, Senator Murkowski's Inbox Privacy Act, S. 759, 106th Cong. (1999), would require junk e-mailers to include identifying data and explicit opt-out provisions in their messages and to comply with recipient requests to cease spamming them. S. 759 would also prohibit junk e-mailers from sending spam to any domain with a no-spamming policy. Congressman Miller's Can Spam Act, H.R. 2162, 106th Cong. (1999), would permit ISPs to sue those who violate their anti-spam policies and would establish criminal penalties for falsifying a domain name on spam.

- **Appendices to "The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet (March 9, 2000)**
- **More Information on: Prosecuting Crimes Facilitated by Computers and by the Internet**

- **More information on: Electronic Commerce**