S. HRG. 108–920

PORNOGRAPHY ON THE INTERNET

HEARINGS

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 9 AND OCTOBER 15, 2003

Serial No. J–108–38

Printed for the use of the Committee on the Judiciary

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00001 Fmt 6011 Sfmt 6011 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

PORNOGRAPHY ON THE INTERNET

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00002 Fmt 6019 Sfmt 6019 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

S. HRG. 108–920

PORNOGRAPHY ON THE INTERNET

HEARINGS

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 9 AND OCTOBER 15, 2003

Serial No. J–108–38

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

93–014 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00003 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
LARRY E. CRAIG, Idaho
SAXBY CHAMBLISS, Georgia
JOHN CORNYN, Texas

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
JOHN EDWARDS, North Carolina

BRUCE ARTIM, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00004 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

CONTENTS

TUESDAY, SEPTEMBER 9, 2003

STATEMENTS OF COMMITTEE MEMBERS

	Page
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	5
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah	1
prepared statement	121
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	2
prepared statement	156
Schumer, Hon. Charles E., a U.S. Senator from the State of New York, prepared statement and attachment	193

WITNESSES

Barr, William, Executive Vice President and General Counsel, Verizon Communications, Washington, D.C.	33
Callaway, Robbie, Chairman, National Center for Missing and Exploited Children, Alexandria, Virginia	11
Hess, Stephen, Associate Academic Vice President for Information Technology, Office of Information Technology, University of Utah, Salt Lake City, Utah	14
Jacobson, Douglas W., President and Chief Technology Officer, Palisade Systems, Incorporated, Ames, Iowa	16
Koontz, Linda, Director, Information and Management Issues, General Accounting Office, Washington, D.C.	6
Malcolm, John, Deputy Assistant Attorney General, Criminal Division, Department of Justice, Washington, D.C.	7
Morris, Alan, Executive Vice President, Sharman Networks Limited, Washington, D.C.	13
Peters, Marybeth, Register of Copyrights, U.S. Copyright Office, Washington, D.C.	36
Sherman, Cary, President and General Counsel, Recording Industry Association of America, Washington, D.C.	30
Spota, Thomas J., Suffolk County District Attorney, Hauppauge, New York	9

QUESTIONS AND ANSWERS

Responses of William Barr to questions submitted by Senators Chambliss, Cornyn and Leahy	43
Responses of Robbie Callaway to questions submitted by Senators Cornyn and Leahy	49
Responses of Stephen Hess to questions submitted by Senator Cornyn	51
Responses of Douglas W. Jacobson to questions submitted by Senators Graham and Leahy	54
Responses of Linda Koontz to questions submitted by Senators Cornyn and Leahy	57
Responses of John Malcolm to questions submitted by Senators Graham, Cornyn, Leahy and Hatch	63
Responses of Marybeth Peters to questions submitted by Senators Cornyn and Leahy	74
Responses of Thomas J. Spota to questions submitted by Senators Graham, Hatch and Leahy	80

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00005 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

Page

Questions submitted to Alan Morris by Senators Hatch, Leahy, Graham, and Cornyn (Note: At the time of printing, after several attempts to obtain responses to the written questions, the Committee had not received any communication from the witness.) 83
Questions submitted to Cary Sherman by Senators Leahy, Chambliss and Cornyn (Note: At the time of printing, after several attempts to obtain responses to the written questions, the Committee had not received any communication from the witness.) 98

SUBMISSIONS FOR THE RECORD

Barr, William, Executive Vice President and General Counsel, Verizon Communications, Washington, D.C., statement 101
Callaway, Robbie, Chairman, National Center for Missing and Exploited Children, Alexandria, Virginia, statement 113
Department of Justice, William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, letter 119
Hess, Stephen, Associate Academic Vice President for Information Technology, Office of Information Technology, University of Utah, Salt Lake City, Utah, statement 124
Jacobson, Douglas W., President and Chief Technology Officer, Palisade Systems, Incorporated, Ames, Iowa, statement 130
Koontz, Linda, Director, Information and Management Issues, General Accounting Office, Washington, D.C., statement 135
Malcolm, John, Deputy Assistant Attorney General, Criminal Division, Department of Justice, Washington, D.C., statement 159
Morris, Alan, Executive Vice President, Sharman Networks Limited, Washington, D.C., statement 170
Peters, Marybeth, Register of Copyrights, U.S. Copyright Office, Washington, D.C., statement 178
Pitts, Hon. Joe, a Representative in Congress from the State of Pennsylvania, statements 191
Sherman, Carry, President and General Counsel, Recording Industry Association of America, Washington, D.C., statement 196
Spota, Thomas J., Suffolk County District Attorney, Hauppauge, New York, statement 213

WEDNESDAY, OCTOBER 15, 2003

STATEMENTS OF COMMITTEE MEMBERS

Page

Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa 221
prepared statement 289
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah 215
prepared statement 292
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont, prepared statement 307

WITNESSES

Buchanan, Mary Beth, U.S. Attorney, Western District of Pennsylvania, Pittsburgh, Pennsylvania 225
Cline, Victor, Emeritus Professor, University of Utah, Sale Lake City, Utah ... 235
Flores, J. Robert, Administrator, Office of Juvenile Justice and Delinquency Prevention, Department of Justice, Washington, D.C. 219
Malcolm, John G., Deputy Assistant Attorney General, Criminal Division, Department of Justice, Washington, D.C. 217
Maxwell, Lawrence E., Inspector in Charge, Fraud and Dangerous Mail Investigations, U.S. Postal Inspection Service, Washington, D.C. 223
Takeshita, Steven, Officer in Charge, Pornography Unit, Organized Crime and Vice Division, Los Angeles Police Department, Los Angeles, California . 237
Taylor, Bruce A., President and Chief Counsel, National Law Center for Children and Families, Fairfax, Virginia 232

QUESTIONS AND ANSWERS

Responses of Mary Beth Buchanan to questions submitted by Senator Leahy . 243

Page

Responses of J. Robert Flores to questions submitted by Senator Leahy 247
Responses of John Malcolm to questions submitted by Senator Leahy 253
A question submitted by Senator Leahy to Bruce A. Taylor (Note: The response was not available at the time of printing.) 260

SUBMISSIONS FOR THE RECORD

Buchanan, Mary Beth, U.S. Attorney, Western District of Pennsylvania, Pittsburgh, Pennsylvania, statements 261
Cline, Victor, Emeritus Professor, University of Utah, Sale Lake City, Utah, statement 270
Flores, J. Robert, Administrator, Office of Juvenile Justice and Delinquency Prevention, Department of Justice, Washington, D.C., statement 273
Hughes, Donna Rice, President, Enough Is Enough, Great Falls, Virginia, statement 294
Malcolm, John G., Deputy Assistant Attorney General, Criminal Division, Department of Justice, Washington, D.C., statement 309
Maxwell, Lawrence E., Inspector in Charge, Fraud and Dangerous Mail Investigations, U.S. Postal Inspection Service, Washington, D.C., statement ... 321
Takeshita, Steven, Officer in Charge, Pornography Unit, Organized Crime and Vice Division, Los Angeles Police Department, Los Angeles, California, statement 329
Taylor, Bruce A., President and Chief Counsel, National Law Center for Children and Families, Fairfax, Virginia, statement 333

PORNOGRAPHY, TECHNOLOGY, AND PROCESS: PROBLEMS AND SOLUTIONS ON PEER–TO–PEER NETWORKS

TUESDAY, SEPTEMBER 9, 2003

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 2:10 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, Chairman of the Committee, presiding.

Present: Senators Hatch, Leahy, Feinstein, Schumer, and Durbin.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Chairman HATCH. Good afternoon. Did they get everybody from outside in? We can put more in who can stand. I think we ought to get as many people in as we can.

In this hearing, we will continue to examine the explosively popular and promising technology which counts among its users millions and millions of teens and pre-teens worldwide, and that is peer-to-peer sharing networks.

At our last hearing on peer-to-peer networks, we examined some of the personal and institutional security risks associated with P2P usage. Today's hearing focuses on a different set of issues and the questions they raise that are equally pressing.

The first panel will address an issue that is very deeply disturbing to me, and I know to other lawmakers as well, the presence on peer-to-peer networks of enormous quantities of pornographic materials, including child pornography, and the great risk of inadvertent exposure to these materials by young P2P users. This is an issue of critical importance to parents, who must be educated about these risks and equipped to control or eliminate them.

The second panel will address the information subpoena provisions of the Digital Millennium Copyright Act, and I will have more to say about that issue after we hear from our first panel.

I know that we here in Congress, along with all upstanding Americans, agree on this: Child pornography is inherently repulsive, inherently victimizing, and intolerable in any form. It is both an effect and cause of sickness. Perverts and pedophiles not only use child pornography to whet their sick desires, but also to lure our defenseless children into unspeakable acts of sexual exploitation.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00009 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

My commitment, Senator Leahy's commitment, and this Congress's commitment to eradicating child pornography was evident in the passing of the PROTECT Act, which Senator Leahy and I cosponsored and helped put through. As we are about to hear, peer-to-peer networks provide a new and growing means for distribution of these disgraceful materials.

They also pose unique challenges for law enforcement, which is trying to combat child pornography, and, of course, unique and unacceptable dangers to our children. The following video presentation conveys the depth and urgency of these dangers. So I would like to complete my opening remarks, before I turn to Senator Leahy, with a showing of this video which was produced by the RIAA, the Recording Industry Association of America, in collaboration with the Suffolk County, New York, District Attorney's Office, which is represented today, the Los Angeles Council on Child Abuse and Neglect, and Media Defender, a security company that has testified repeatedly before Congress and before this Committee.

I should warn you that some of the language in this video is graphic and the content is disturbing. But this is just an example of what our children are witnessing on peer-to-peer networks, and we need to know about it. An edited transcript will be prepared for the record.

[The prepared statement of Senator Hatch appears as a submission for the record.]

So if we could have the video presentation, then I will yield to Senator Leahy for his remarks.

[Videotape shown. Being retained in Committee files.]

Chairman HATCH. Senator Leahy, we will turn to you.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Thank you, Mr. Chairman.

At the first Committee hearing on peer-to-peer networks back in June, we considered the significant dangers that file-sharing can pose to users' privacy and the security of their computers, the fact that they can take up everything from your health records out of your computer, to your children's school reports, and so forth.

Today, we are going to explore possible solutions to some of the problems raised by peer-to-peer networks and online file-sharing. I really feel that unless we find some of these solutions, peer-to-peer is never going to realize its enormous potential to build online communities, to enhance network learning, to make unprecedented amounts of material, educational and entertaining, available worldwide. These are all the good things that can be done in peer-to-peer sharing, certainly not what is seen by any of us in this room in those things we have just seen in the video.

I believe that peer-to-peer has the potential to revolutionize the way we share our information. But like any technology, it can be and is being abused. Peer-to-peer networks can delve into people's private records, as I said earlier. You share music or whatever else and you may end up also picking up everybody's tax returns or their Social Security numbers, their credit card numbers or anything else. Of course, we know that it is used often to illegally share copyrighted material.

But I think even beyond that, the most disturbing thing is what we have just seen in the Chairman's video. Peer-to-peer networks can be used to distribute child pornography and to make all sorts of pornography available to unsuspecting children, something, Mr. Spota, your office has looked into a great deal.

If peer-to-peer networks are going to be part of our culture, they have to respond to these problems. We certainly can't allow those who purposefully exploit network file-sharing to harm children—we can't allow them to go unpunished; we really can't. I think that is something everybody on this Committee of either party will agree to.

As a father, and now blessed to be a grandfather, I find child pornography despicable. There is no Senator up here who disagrees with this. On this Committee, the Chairman and I working together—at times when I was Chairman and times when he has been Chairman, we have worked together to take strong steps to protect our children from pornography, and we will do everything possible to combat child pornography.

As a former prosecutor, I want to see that law enforcement has effective tools for the identification and prosecution of individuals who make, use, and traffic in this material.

Pornography, especially child pornography, is prevalent on peer-to-peer networks. As much as 42 percent of peer-to-peer requests are for pornography. A recent GAO study on that, I believe, is a wake-up call for our country. They found that simple keyword searches on a peer-to-peer network turned up hundreds of pornographic images of children. In fact, when GAO did that search, they found that 40 percent of these searches turned up child pornography.

The National Center for Missing and Exploited Children, which I might say continues to do outstanding and inspirational work to protect all of our children, reports that there has been a four-fold increase in pornography on peer-to-peer networks in just 1 year.

I think I am right on that, am I not, Mr. Callaway?

Mr. CALLAWAY. Yes.

Senator LEAHY. Moreover, peer-to-peer networks don't simply allow the distribution of child pornography. Through the use of instant messaging, what I worry about very much is that it can be used to lure children into meetings with sexual predators.

So far, the peer-to-peer networks are not only turning a blind eye to this problem, but in many cases they are specifically designed so that parents are unable to keep their children off the network with a traditional firewall. Every parent ought to be able to have a traditional firewall so they can keep their children off this. Every parent would want to.

In addition, what few protections are available are designed so they can be easily circumvented by a child regardless of their parent's intentions. After all, a teenage child is probably far more knowledgeable of how to use that computer than the parent is.

More disturbingly, the networks are actively hindering law enforcement efforts to crack down on child pornography. Even though it has risen, as I said, four-fold between 2000 and 2002, arrests for child pornography have dropped dramatically in recent years. We have heard that one, and perhaps the only reason for this is that

peer-to-peer networks have changed their systems to allow their users to remain anonymous.

In their zeal to allow illegal file-sharing, the networks have made it far too difficult for law enforcement to track down child pornography, and that has to stop. Believe me, if it is possible for legislation to do it, we will.

So I look forward to hearing from the outstanding group of experts who are here today on the steps that can be taken to stop child pornography. It is best solved by the people who understand it and deal with it on a daily basis. We can write all kinds of legislation here, but in a fast-changing world with the science, electronics and everything else changing so quickly, it is the people who deal with it everyday that, if they want to, can stop this because they are the ones that have the tools. I would like to see a private sector solution to this very serious problem. Make no mistake, it has to stop, and if it can't stop by the private sector doing it, then we will have to take steps to make it stop.

One of the panels will look at one of the solutions to online file-sharing that we enacted 5 years ago as a part of the Digital Millennium Copyright Act. Senator Hatch and I worked for months, actually for years, I think, on that one—

Chairman HATCH. Five years.

Senator LEAHY. —to get tools in the fight against online copyright infringement. At the time we were drafting the DMCA, the recording industry, the Internet service providers, and others said they were having trouble identifying individuals who might be illegally sharing copyrighted materials online.

The parties came together and they determined that the best solution was to allow copyright-holders to subpoena the information, and Section 512(h) codified that. Now, I understand that this section is being used to subpoena information about individual users who may be sharing copyrighted materials, but who are not using the ISP system or network to store it.

In short, it is being used to combat the anonymous use of peer-to-peer networks. There can be little doubt that use of the 512(h) subpoena raises legitimate concerns for some, such as notice to the end user, and so on. Again, the people working on this are the ones best able to solve it.

I would say there is somebody here from the Department of Justice. I have recently sent a letter to the Attorney General. We are still waiting for the regulations on the internet service providers' duty to report child pornography to the National Center for Missing and Exploited Children, and I would urge the Attorney General and the Justice Department to get us those regulations. It could be a powerful tool.

Mr. Chairman, I have taken longer than usual, but you and I have worked on this for so many years and it is aggravating in trying to find a solution.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Chairman HATCH. It is an important subject and I appreciate your statement, Senator Leahy.

Our first panel of witnesses is comprised of seven witnesses and they are Linda Koontz, the Director of Information Management

Issues, United States General Accounting Office; John Malcolm, Deputy Assistant Attorney General of the Criminal Division, U.S. Department of Justice; Thomas Spota, the District Attorney for Suffolk County, New York; Robbie Callaway, Chairman of the National Center for Missing and Exploited Children; Alan Morris, Executive Vice President of Sharman Networks, distributor of Kazaa Media Desktop; Stephen Hess, Associate Academic Vice President for Information Technology at our own University of Utah; and Douglas Jacobson, President and Chief Technology Officer of Palisade Systems.

I am grateful to have all of you here. I would like to thank Mr. Malcolm for kindly agreeing to appear on this panel along with our private sector witnesses rather than on his own panel. That will expedite this hearing quite a bit. I would like to thank all of you for taking the time to be with us here today to discuss these important issues.

Before we begin, Senator Feinstein, do you have any comments you would care to make?

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. I have just been reading the GAO report on this subject, Mr. Chairman. Thank you. I must say I am really astounded at the film we just saw, the use of Pokemon to be able to pull up child pornography, the use of the words "Harry Potter" to be able to pull up child pornography.

It seemed to me that one of the people in this really had the solution, and that is that the operators have a responsibility to see that this doesn't happen. I think what I have heard so much of is that, oh, nobody can control the Internet. It is like telephones; there can be no restrictions, no regulations. But it is really not like telephones.

I think this piece of film that you showed, Mr. Chairman, was really worthy of oversight. It seems to me that we ought to find a way to prohibit, perhaps on the basis of copyright, use of words like "Pokemon." I am sure the copyright owners would not want Pokemon used that way, nor would Harry Potter's copyright want Harry Potter used that way.

I don't know about the prohibition of downloading of these things, but I think we ought to look into it, and I think we ought to perhaps try to prohibit free access of copyrighted material. But I think one thing is clear that this is like a growing cancer, and increasingly when you have people arrested on charges of child molestation, police are finding in their rooms electronic pornography, as well as other pornography. So there is a nexus increasingly, I believe, between the two.

I think the argument has been made throughout the years that what this does is reinforce a person of low maturity with the ability to commit this kind of act in real life. So I think it is a very real and considerable danger to our young people and that we have an obligation. I would just like to offer my help to both you and Senator Leahy in this regard.

Chairman HATCH. Well, thank you so much, Senator.

Now, on your microphone there is a button right in front. When you push it, it turns a little bit red, so that will mean you are on. So remember to push it before you start speaking.

We will turn to you, Ms. Koontz, first.

STATEMENT OF LINDA KOONTZ, DIRECTOR, INFORMATION AND MANAGEMENT ISSUES, GENERAL ACCOUNTING OFFICE, WASHINGTON, D.C.

Ms. KOONTZ. Mr. Chairman, Senator Feinstein, thank you for inviting us to discuss our work on the availability of pornography on peer-to-peer networks. We provided the results of this work in a report to the House Committee on Government Reform in February of 2003. This report contains additional details on our methodology and our results, and I would ask to submit it for the record.

Chairman HATCH. Without objection.

Ms. KOONTZ. To summarize, I will provide some background on peer-to-peer networks and discuss the ease of access to child pornography on peer-to-peer networks and the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography.

Just to briefly review some of how peer-to-peer networks are configured, our first chart shows the two main models of peer-to-peer networks. On the left is the centralized model. A centralized server or broker maintains a directory of shared files stored on the computers of users and directs traffic between the users.

The centralized model was employed by Napster, the original peer-to-peer network. Because much of the material traded was copyrighted, Napster, as the broker of these exchanges, was vulnerable to legal challenges which led to its demise last year.

The right side of the chart shows the decentralized model, which is currently used by the most popular peer-to-peer networks. In this model, individuals locate each other and interact directly.

In work we conducted earlier this year, we found that child pornography, as well as other types of pornography, is widely available and accessible through peer-to-peer networks. We used Kazaa, a popular peer-to-peer file-sharing program, to search for image files using 12 keywords known to be associated with child pornography on the Internet. As shown on our chart, of over 1,200 items identified in our search, about 42 percent of the file names were associated with child pornography images, and about 35 percent were associated with adult pornography.

In another Kazaa search, we worked with the Customs CyberSmuggling Center to use three keywords to search for and download child pornography image files. As you can see on our next chart, this search identified 341 image files, of which about 44 percent were classified as child pornography and 29 percent as adult pornography.

More disturbingly, we found that there is a significant risk that juvenile users can be inadvertently exposed to pornography, including child pornography. In searches on three innocuous words likely to be used by juveniles, we obtained images that included a high proportion of pornography. As you can see on the chart, almost half of the 177 retrieved images were classified as pornography, including a small amount of child pornography.

Mr. Chairman, Internet file-sharing programs are rapidly gaining users, and while there are no hard statistics, it is thought that a large proportion of these users are juveniles. These programs provide easy access to pornography, including child pornography. Further, our work shows that such networks put even the youngest users at risk of being inadvertently exposed to pornography.

In light of these factors, it will be important for law enforcement to continue to devote effort to peer-to-peer networks and for policymakers to continue to highlight this issue to parents and to the public, and to lead the debate on possible strategies for dealing with it.

That concludes my statement. I would be happy to answer questions at the appropriate time.

[The prepared statement of Ms. Koontz appears as a submission for the record.]

Chairman HATCH. Thank you, Ms. Koontz.

Mr. Malcolm, we will turn to you.

STATEMENT OF JOHN MALCOLM, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. MALCOLM. Mr. Chairman, Senator Leahy, Senator Feinstein, thank you for inviting me to testify before you today on this critical topic.

The sexual abuse of a child is a horrific act which is often exacerbated by pedophiles who memorialize their repugnant crimes in photographs and videos. Sadly, with increasing frequency, such offenders are disseminating these grotesque memorials to millions of people over the Internet.

Law enforcement must respond to technological advances, eradicating child pornographers from every forum in which they lurk, whether in cyberspace or elsewhere. Thus, I commend you for holding this hearing on the proliferation of child and adult pornography on peer-to-peer networks.

In contrast to traditional networks, peer-to-peer networks are less centralized. In fact, they are fluid by design. While a traditional network operates like a bicycle wheel in which a central server computer is the hub that sends out files through the spokes to smaller computers arrayed along the tire, peer-to-peer networks act more like a fisherman's net. Each peer computer is connected to the rest of the peer computers either directly or through one or more intermediary computers.

In a P2P network, files are kept not on a central server, but rather on each of the peer computers hooked into the network at any given point in time. Any computer can be utilized to download peer-to-peer software from the Internet and thereby gain access to shared files located on other computers connected to the network. Once the software is installed, peer-to-peer networks can be accessed to transfer virtually anything that can be put into digital form, including pictures, music, or videos.

Once the user selects the files he wishes to download, the source and destination peer computers exchange the files directly. Similarly, a user can also elect to share certain files on his own computer with other users on the peer-to-peer network. Given this for-

mat, it is very easy and not surprising that this medium has become a hotbed of criminal activity, including the dissemination of child pornography.

Congress is well aware that adult pornography is readily available to children on the World Wide Web and is often inadvertently accessed by children using innocuous search terms such as the names of cartoon characters or children's television shows.

Indeed, to combat this growing problem, Congress through the PROTECT Act recently enacted a law criminalizing the use of domain names that mislead minors into viewing harmful material. Despite the potency of this new legislation, it does not extend to file names that individuals create for files on their own computers that they choose to share over peer-to-peer networks.

Thus, any child who downloads peer-to-peer software and enters an innocuous search term—a pop star, a cartoon character—may be confronted with files containing adult pornography that have been given misleading names. Similarly, by entering fairly blatant terms that are well-known to pedophiles, such as "child porn," "preteen," or "lolita," a user, perhaps an unsuspecting child, will receive child pornography that is easy to access and download.

Because peer-to-peer networks operate as a diffuse community of computers, the investigation of child pornography offenses in the peer-to-peer context requires a proactive and focused approach by law enforcement. The lack of a central server means that there is no clearinghouse for files and information that can serve as a bottleneck or choke point where law enforcement can gather logged evidence and illegal activity can be cut off.

Moreover, the decentralized nature of peer-to-peer networks means that there is no central community in which people chat about their illegal activity. In addition, many peer-to-peer networks do not require individual users to set up accounts with a central authority. Peer-to-peer users can change their names at will and the names that they choose rarely contain true information that would identify them.

Nevertheless, just as an individual cannot receive or place a telephone call without a telephone number, every instance of Internet access is associated with an Internet protocol or IP address. Thus, using peer-to-peer software, a law enforcement agent can identify a file containing child pornography and, while downloading that file, identify the IP address of the user who sent it. The agent can then serve the Internet service provider with process and thus ultimately obtain the identity of the person who uploaded that file.

Moreover, the seizure of a user's computer will often contain fruitful evidence to use for further investigation. Thus, while it is true that people can do a lot to hide their identities, nobody is truly anonymous who uses a peer-to-peer system.

Notably, however, new generations of peer-to-peer file-sharing protocols are promoting for their users even greater anonymity, including the ability to hide behind proxy servers and the like. When this technology comes to fruition, it is going to present significant challenges to law enforcement.

While there is no question that there is a lot of pornographic and obscene material on peer-to-peer networks, it is difficult to quantify the percentage of child pornography on peer-to-peer networks. As

you have just heard, with search terms, sometimes you get a lot of child pornography if the term is one that a pedophile would use. If you use an innocuous term, you will get less.

For reasons that are discussed in greater detail in my written testimony, in fact, while there is a lot of child porn on peer-to-peer networks, purveyors of this material tend to use other mediums such as news groups and Internet relay chat rooms. Nonetheless, the Department of Justice is vigorously committed to prosecuting any child pornographer, no matter what forum they use. The Child Exploitation and Obscenity Section and its high-tech unit and U.S. Attorneys' offices across the country are vigorously involved in that pursuit.

Mr. Chairman, I again thank you and this Committee for inviting me to testify here today and I look forward to answering your questions.

[The prepared statement of Mr. Malcolm appears as a submission for the record.]

Chairman HATCH. Thank you so much.

Mr. SPOTA.

Senator LEAHY. If I might, Mr. Chairman, urge Mr. Malcolm to get us those regulations from his Department. It would be very, very helpful in this fight.

Mr. MALCOLM. Yes, sir.

Chairman HATCH. Mr. Spota.

STATEMENT OF THOMAS J. SPOTA, SUFFOLK COUNTY DISTRICT ATTORNEY, HAUPPAUGE, NEW YORK

Mr. SPOTA. Thank you, Mr. Chairman and members of the Committee. I appreciate the opportunity to appear this afternoon to discuss the issue of child pornography on peer-to-peer file-sharing networks and the efforts of those of us in Suffolk County to combat what we view as a growing concern for law enforcement nationwide.

Earlier this year, I was so disturbed by information brought to my attention about the nature and accessibility of child pornography on peer-to-peer networks that I authorized the commencement of an investigation by members of my staff, the D.A.'s office, as well as the Suffolk County Police Department, into Kazaa, a popular file-sharing program.

I was amazed that the file-sharing programs used by so many of our children and adolescents to download music were also the repository of some of the most graphic child pornography available today.

There is no special code or unique search term required to unlock the key to child pornography in these networks. If you search for songs by artists as popular as Brittany Spears, the Beatles, or Pokemon, if you are looking for any song or any movie with the word "young" as part of its title, your search results will most certainly include child pornography. The names of the files are disturbing enough, but a simple click of the mouse is all that is necessary for anyone, including any of our children, to be exposed to the dark, disturbing, and violent world of child sexual abuse.

Working in conjunction with the Suffolk County Police Department Computer Crimes Section, the investigation conducted by my

office relied upon sophisticated computer technology and, quite frankly, good old-fashioned police work. Numerous grand jury subpoenas were issued to Internet service providers, and based on the information received search warrants were executed upon residents of Suffolk County and computers, CDs, and other storage media were seized.

Police officers, who are also forensic computer analysts, evaluated the seized evidence and recovered hundreds of images of child pornography. I then presented evidence to a grand jury that resulted in the indictment of 12 Suffolk County residents for over 180 counts of the possession and promoting of child pornography.

The images of child pornography available on peer-to-peer networks are some of the worst seen by law enforcement to date. Included in the images seized by police in our case and the cases being prosecuted by my office are still photographs of very young children engaged in sexual acts with other children and adults, and video clips lasting several minutes of children being subjected to unspeakable acts of sexual violence.

Some of those video clips have sound, and in one case, as we saw in the video, there is a child being heard saying "No, Daddy, stop, no, Daddy," in a futile attempt to prevent being raped. In another instance, we saw very clearly the diapers of a child being removed before the child's father or whoever it was sexually manipulated that infant.

To say that this is disturbing is an understatement. Not only does every image represent the sexual assault of a helpless child, but the use of a medium such a peer-to-peer network allows the assault to be broadcast worldwide and revictimizes the child each and every time the image is viewed.

Today, it is not uncommon for a child to report to us, to law enforcement, that their abuse had been video-recorded, and later for those very same images to turn up in the forensic examination of a computer in a totally unrelated case. Thus, the child's abuse will be available forever on the Internet or on a peer-to-peer network. And how devastating this must be for a child to know or come to understand that his or her victimization is available to the world in perpetuity.

Congress should act to make peer-to-peer file networks and their operators responsible for the child pornography available to their users. Law enforcement activities can serve to punish offenders and educate the community, but they will never be enough to ultimately stem the tide. We must do more to educate and inform American parents.

Seasoned child abuse prosecutors in my office and elsewhere were unaware of the capability of Kazaa to file-share child pornography until we began our investigation. I wonder how many other parents are unknowingly putting their children at risk by allowing them access to a program they believe is harmless.

Americans employ a rating system for movies and TV shows to protect children. Compact discs contain parental advisories. Kazaa and other programs like it have no such warnings and seem to have total immunity, and I say this is wrong.

As far as I am aware, I am the only district attorney on a State level to investigate and prosecute users of a peer-to-peer file-shar-

ing network for the possession and promotion of child pornography. The case has generated considerable interest from other State law enforcement agencies and I hope they will initiate similar prosecutions.

Our investigation is continuing in the hopes of identifying some of the perpetrators of these horrific acts, and the children so that they can be protected from further abuse. As a standard protocol, the images will be forwarded to the National Center for Missing and Exploited Children to aid us in this endeavor.

I thank you again for inviting me to speak to you on this important issue.

[The prepared statement of Mr. Spota appears as a submission for the record.]

Chairman HATCH. Well, thank you, Mr. Spota. We appreciate the efforts you are making in this regard.

Mr. Callaway, we are always happy to welcome you before the Committee, so we will turn to you at this time.

STATEMENT OF ROBBIE CALLAWAY, CHAIRMAN, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, ALEXANDRIA, VIRGINIA

Mr. CALLAWAY. Thank you. It is good to see you, Mr. Chairman, Senator Leahy, Senator Feinstein. It is good to be back in front of you on this tough issue. If I could, if it wouldn't break protocol, I would ask for a round of applause for this district attorney, for that testimony and what he has been doing on this issue. We need more like him.

[Applause.]

Mr. CALLAWAY. The National Center, as you know, has been in the forefront of this issue on child pornography for nearly two decades. You have my formal testimony. I am going to sum it up very quickly.

Since 1987, the National Center has operated the National Child Pornography Tipline in partnership with the U.S. Customs Service and U.S. Postal Inspection Service. Since 1998, we have operated the CyberTipline, a 24-hour online mechanism for reporting child pornography and other sexual exploitation crimes, handling 150,000 leads, including just over 1,500 reports regarding child pornography being traded by P2P users.

Senator Feinstein and all of you know that I work for Boys & Girls Clubs of America. My volunteer work is the National Center. This is not even what I was going to talk about, but as they talked about the search names, we had a demonstration where they go and look for search names. You talk about Pokemon or you talk about Brittany Spears.

If a young boy at the Boys & Girls Club in Salt Lake City were to be going to visit a cousin, let's say, at the Boys & Girls Club in Burlington, Vermont, he might get on the Internet and he might look it up. He might look in one of these file-sharing systems and look up Boys & Girls Clubs to find out if there is a Boys & Girls Club in Vermont. You would be shocked at what comes before you when you look up a Boys & Girls Club. So we are quite concerned about that from our Boys & Girls Club hat as well.

The National Center's primary concern regarding file-sharing is that it has become virtually impossible to track down the people who are doing it. From the National Center data and interaction with leading law enforcement investigators, we have concluded that the use of file-sharing programs to trade, distribute, and disseminate child pornography is significant and growing dramatically.

Yet, in file-sharing programs, law enforcement lacks the necessary tools to identify and track down many perpetrators. This lack of necessary tools is allowing for major growth among those who distribute illegal child pornography.

The National Center is particularly concerned about the inadvertent exposure of children to such content, just as I said, if they were to go to look for Boys & Girls Clubs or if they go to look for Pokemon or whatever. The Center urges parents to get involved and stay involved in what their children are doing on the Internet and on the computers.

We can all agree that children who are involved in child pornography are by their very nature of the industry victims of child exploitation and sexual abuse. Ann Burgess, of the Boston College Nursing School, states, and I quote, because I was asked about the effects on children—Ann Burgess says, "The destructive effects of child sexual abuse can create a number of long-term problems for the child victim, including headaches, stomach aches, and sleeping and eating disorders, psychological reactions of fear and anxiety, depression, mood changes, guilt, shame, social problems with school truancy, declining grades, fighting, sexual problems, preoccupation with sex and nudity, and running away from home." All of these are issues that I have testified about to this Committee regarding juvenile justice legislation. "Substance abuse, gender identity confusion, sexual dysfunction, and social deviant behaviors have also been identified as possible consequences of untreated childhood sexual abuse," end of quote.

To summarize, the National Center believes the use of peer-to-peer networks for the distribution of pornography is a growing problem and we are asking for your help. Based on our own review of CyberTipline leads and information in our work with leading law enforcement investigators across the country, we are convinced that P2P has become a major growth area for those desiring to trade or distribute illegal child pornography with little risk of identification and prosecution.

Peer-to-peer program developers could make great strides in protecting children if they permitted software programmers to allow users to log the origination of all files. We need to make sure that law enforcement has the necessary tools to identify these perpetrators, and use them to identify, arrest, and prosecute, and in so doing protect our children.

Mr. Chairman, let's be very clear about my position because some people say, well, why are you doing it, why are you here? Our position is this—and you have heard me say it before—when you make child pornography, you commit a crime. You commit a crime against not only the child involved in the child pornography, but against all God's children.

When you view child pornography, you are committing a crime. There is no socially-redeeming value for child pornography anywhere, any time, anywhere in the world. And when you share a file of child pornography, you have committed a crime. We need to be able to prevent child pornography from being made, and we need to be able to prosecute anybody who shares a file of any type of child pornography.

Thank you very much.

[The prepared statement of Mr. Callaway appears as a submission for the record.]

Chairman HATCH. Thank you, Mr. Callaway.

We will turn to you, Mr. Morris.

STATEMENT OF ALAN MORRIS, EXECUTIVE VICE PRESIDENT, SHARMAN NETWORKS, LIMITED, WASHINGTON, D.C.

Mr. MORRIS. Thank you very much, indeed. Like all other parents in this room, I utterly abhor child pornography and applaud what you just said. I totally agree with that. I would do anything to protect my children from child pornography.

Senator Hatch and members of the Committee, when you invited me at the end of last week to come over here, I had no hesitation in jumping on a plane and coming straight over. The issue is important.

As you know, I am the Executive Vice President of Sharman. I am responsible particularly for the distribution of licensed content. We are the world's largest distributor of licensed content. Sometimes, our best is not good enough, and as far as child pornography is concerned, we will do whatever it takes to ensure that child pornography reduces from the level it is on peer-to-peer.

Let me tell you very briefly what we have done so far. Firstly, when we acquired the Kazaa Media Desktop in January 2002, we ensured there was a family filter, enabled by default, when the program is downloaded. Now, that family filter blocks abusive and offensive terms. The terms are culled from the Internet, because we know from your own data this is where most child pornography originates. There is the option for the parent to put additional terms in and this may be further password-protected.

Secondly, we cooperate with law enforcement agencies. I am responsible for dealing with law enforcement agencies, and to date only 4 in the last 18 months have contacted us. We have spoken at a senior level, however, with the FBI because we are not satisfied with the fact that the amounts may be relatively low and diminishing.

I understand very well, as people have pointed out, that on peer-to-peer we cannot know what files are transacted. However, what we have done is to work with and to identify third-party applications which they can use very much in the manner you just suggested to track IP addresses.

It has been very important to us that while we protect the privacy of users from harassment, et cetera, that we don't block or hinder in any way legitimate law enforcement agencies finding IP addresses. So as a matter of record, we do not have anonymizers, we do not use proxy servers. We think that is not necessary. In the

community of sharers around the world we are trying to build, there is nowhere for pedophiles to hide.

I am a little bit confused because in the New York Times on Sunday, we saw some data that came from the National Center for Missing and Exploited Children which seems to indicate that the level of pedophile material on file-sharing networks is relatively small, less than 3 percent, and declining. Be that as it may, any material is too much.

We are not prepared just to rest. As I said, we want to reduce it to zero. We have in development technical measures that will make it even harder for this material to circulate. When they become available, Mr. Chairman, in the confidence of yourself and your Committee, we will discuss them with you, but obviously we wouldn't discuss them publicly.

The other thing which is very important—and again people have alluded to it—is education. We all know that filters are not perfect. We also know that people are not very good about computer security. We know they don't use anti-virus protection, we know they don't use their passwords properly. So a program of education is something we think is very important. Together with the Distributed Computer Industry Association, we are working on a program of education, and if there is anybody here today that wants to work with us, we are very happy to do so.

This, as people have suggested already, is an Internet problem. If you enter the most commonly used search word on Google, an eminently respectable search engine, you will get 40 million search results. And I needn't tell you that term is an adult and very explicit term. So this is an industry-wide issue.

I was very surprised to see that Hollywood has a view on this. It has been suggested, and indeed it was in the New York Times and the L.A. Times that this is a cynical plot by Hollywood to further their own commercial ends. Be that as it may, we have a zero-tolerance policy—it is that simple—for pedophilic material, and we will not be happy until it is eradicated completely.

I now offer our services to any of the members of this panel to work with them, indeed work with you, Mr. Chairman, to do two things; one, to reduce the amount of pedophile material down from the 2 or 3 percent it shows here to zero; and, secondly, a program of education so that parents can exercise their responsibility to use the password-protected filter, and to also enjoin the rest of the Internet to do the same.

Mr. Chairman, thank you very much.

[The prepared statement of Mr. Morris appears as a submission for the record.]

Chairman HATCH. Thank you, Mr. Morris.

Mr. Hess, we are delighted to have you with us today.

STATEMENT OF STEPHEN HESS, ASSOCIATE ACADEMIC VICE PRESIDENT FOR INFORMATION TECHNOLOGY, OFFICE OF INFORMATION TECHNOLOGY, UNIVERSITY OF UTAH, SALT LAKE CITY, UTAH

Mr. HESS. Senator Hatch, Senator Leahy, and other distinguished members of the Committee, I work for the University of Utah. We are located in Salt Lake City, Utah. We have an enroll-

ment of about 28,000 students, and part of the role of the University of Utah is to also provide Internet access to all public schools within the State of Utah. So you might say we are a large ISP serving the State.

You have a written copy of my testimony which details most of the information and experience that we have had with peer-to-peer, but I was told in this testimony to give you some of the experiences that we have as a network operator in dealing with peer-to-peer relationships, and more specifically in the area of pornography.

I would like to make a few points. Number one, because universities are research and information enterprises, IT has become a very essential part of what we do. It is, in effect, our central nervous system. It holds potential for great efficiency during a time of rising costs and greater accessibility to education and research, free from the constraints of time and place.

Number two, peer-to-peer has great potential in sharing information and helping in that education enterprise. We hope in the resolution of copyright and the issues discussed here today that peer-to-peer technology can be preserved, along with emerging technologies, in support of learning and scholarship.

Number three, but we understand that there are two sides to this issue and are dismayed by the inappropriate uses of this technology. Unfortunately, it has been used for the sharing of copyrighted material, pornography, and now viruses and worms. The abuse of this technology has also taken a great amount of our computing capacity and IT personnel time, which are all designated for educational purposes. In our attempts to technically block or restrain this activity, some developers of peer-to-peer technologies have initiated clever upgrades to stop us from blocking this inappropriate traffic.

Number four, the university is placed in a difficult position, of trying to find a balance between the enabling of a promising new technology while discouraging inappropriate, illegal, or threatening behavior. We welcome any thoughtful discussion on these policies and practices that can minimize our already overburdened IT staff.

Number five, we recognize our role to establish and uphold community standards which are reflected in our university policy. We go to great lengths to educate end users on legal, ethical, and appropriate use of computing resources. We promote fair use of online digital content, and thank this Committee and Congress for the wonderful TEACH Act which was passed a few months back. The university considers illegal sharing of copyrighted materials and the downloading of pornography as a violation of our IT acceptable use policy.

Number six, to comply with the law and our acceptable use policies, and to protect our networks and computing resources, we have to balance privacy with compliance. We do this in the follow way.

First, we monitor traffic flows, but not for content. Traffic flow is a measure of the amount of data transmitted over a network. Content is information contained within the data flow. When an excessive data flow is detected or is seen over the network, it can bring down the network. This, in turn, brings down the hundreds of thousands of applications that run on our networks vital to the day-to-day, hour-by-hour operation of the Internet.

When excessive traffic is detected, we contact the end user to see if the use of the network is legitimate. Some of these excessive flows come from peer-to-peer sharing of copyrighted materials and the downloading of pornography. If these people are downloading pornography or downloading copyrighted material, in violation of law, they are cut off our networks until they come in compliance with the policy.

Second, we may also receive notification from copyright-holders about violations of end users. We may be notified by a department Chair, dean, or vice president about violations as well. In these cases, if the violation of copyright is involved or the downloading of pornography, people, by policy, are cut off from the network and must go through an education process to be reinstated. We have yet to have repeat offenders.

Number seven, pornography is not acceptable use of university IT networks and resources unless it is used for academic or research purposes. If faculty, staff, or students are found to possess illegal pornography, they are deemed to be in violation of Federal and State laws and are reported to law enforcement agencies.

While technologies like peer-to-peer can be disruptive, they continue to provide the opportunity to advance civilized life in a democratic and open way. We support a flexible and balanced approach to keeping technology open and better able to serve the public, but deal with the people who abuse these systems.

Thank you.

[The prepared statement of Mr. Hess appears as a submission for the record.]

Chairman HATCH. I was very interested in what you are doing up there. It is amazing.

Mr. JACOBSON.

STATEMENT OF DOUGLAS W. JACOBSON, PRESIDENT AND CHIEF TECHNOLOGY OFFICER, PALISADE SYSTEMS, INCORPORATED, AMES, IOWA

Mr. JACOBSON. Mr. Chairman and members of the Committee, I would like to thank you for the opportunity to appear here today and discuss the issues surrounding peer-to-peer networks. A more detailed discussion of these issues can be found in my written testimony.

By way of introduction, I am Associate Professor of Electrical and Computer Engineering at Iowa State University and Director of Iowa State's Information Assurance Center. At the same time, I also serve as President and Chief Technology Officer of Palisade Systems, a company which has developed products to help deal with peer-to-peer file-sharing.

You don't have to look for pornography on peer-to-peer networks. As many of our panelists have talked about, you just type in a search string and it finds you. You can even type in a name of a file that you know doesn't exist on the network and you will come up with peer-to-peer pornography that will match that file. I did this in a class I taught, and it turns out there are actual programs on the Internet, on these peer-to-peer networks that will generate matches to your files and return links to pornography. So you don't even have to have a file out there.

Palisade Systems conducted a study of searches on the Gnutella network, which is a peer-distributed network, and our studies are in line with other studies showing 42 percent of the requests were for pornography; 6 percent of those requests were for child pornography. Many other studies have been published, all coming to the same conclusion. An argument can be made that legitimate peer-to-peer applications would not need to hide from detection or evade monitoring, as was pointed out by Mr. Morris.

I want to talk briefly about the ways that these protocols have evolved over time to circumvent the methods that administrators have used to block them. First there was port-blocking. The early peer-to-peer protocols ran on certain ports and administrators blocked those ports. The peer-to-peer protocols quickly evolved to do port-hopping, so the port numbers would change in order to avoid detection.

When administrators locked their networks down even further so that they only allowed a few critical services, these peer-to-peer applications began using a technique called tunneling, where they pretended to be legitimate applications. They would start to look like Web traffic or other types of legitimate traffic. So these protocol, are evolving, trying to avoid being detected.

I will talk briefly about some additional filtering techniques. Another filtering technique beyond port-blocking is something called signature-based, where you actually look at the way these protocols communicate. Palisade Systems, for example, has a product that works this way, and so it is sort of like virus detection.

There is content-based filtering, where you try to look at the content of the data and actually determine whether the data is copyrighted material or potentially a material that is of an illegal nature. This turns out to be very difficult to do, especially if the material can't be cataloged, like pictures of pornography. There is no catalog of all the images. Again, the peer-to-peer networks are now moving to encryption in order to hide all the data that they transfer.

A final method is something called white-listing, where you allow only those things that you know are good, only those protocols you know are good, and block all other types of traffic.

As I have said, these protocols are evolving and the newest steps in the evolution are that of encryption and anonymous access. The best example of this evolution is the newest application called Earthstation 5. This protocol uses both encryption, anonymous access, and tunneling. The website for Earthstation 5 makes it clear they are working at efforts to stop filtering of the protocol.

A couple of observations can be made from the review of these filtering technologies. While each technology has certain limitations, using multiple technologies in a layered approach seems like the best defense in a corporate environment. However, this method often requires knowledgeable staff and constant monitoring of the networks.

Second, most technologies are focused on a corporate market and are not designed for home users. If a home user allows these applications to be installed, little can be done to prevent downloading of pornography or other material. This leaves the home user with

no choice but to either allow peer-to-peer activity and all its associated risks or try to set up a way to not allow any of it.

It should be possible for Internet service providers to offer a service that blocks all peer-to-peer traffic similar to the way they offer a service for web filtering. The bottom line is the home user needs to be educated about the potential dangers of peer-to-peer networking.

In summary, I have outlined how peer-to-peer networking has evolved to avoid detection and filtering. I see no signs of this evolution slowing down. In fact, with the advent of the newest protocols like Earthstation 5, we will be facing increasing challenges over the years ahead.

Also, given the inherent distributed nature of the peer-to-peer protocols and the difficulty in identifying these networks, I predict that peer-to-peer networks will become a method of choice to distribute illegal materials across the Internet. Companies like Palisade Systems, in conjunction with research universities like Iowa State University, will continue to develop new technologies to combat the evolution of these peer-to-peer networks.

I would like to thank you for the opportunity to testify and I am pleased to answer any questions.

[The prepared statement of Mr. Jacobson appears as a submission for the record.]

Chairman HATCH. Well, thank you so much.

Let me just begin with Mr. Spota and Mr. Malcolm. What can law enforcement do or what can we do here in the Congress to help you to eradicate pornography from these networks? What would be your suggestion?

Mr. SPOTA. If I may, Senator, the way I see it, I can do nothing other than to prosecute those within my jurisdiction, which would be on a country level within the State of New York, Suffolk County, State of New York. I have a staff of 161 prosecutors. I probably could ask every single one of them to devote each and every hour and we would never be able to eradicate this. We would be doing nothing other than trying to put some dent in the County of Suffolk itself, where either possessing or promoting this—people can be brought to the bar of justice by my office. It just seems to me that it has to be done on a Federal level.

As I indicated before, where you have distributors and these networks which are reaping enormous profits, something should be done. They must bear some responsibility, and it seems to me that anything that has to be done should be done by Congress to give our Federal law enforcement counterparts all the tools necessary to have the jurisdiction to reach these people. That is the way it seems to me it can be done. The specifics I can't give you, but perhaps Mr. Malcolm can. But it has to be done on a Federal level

Chairman HATCH. Mr. Malcolm, what would you suggest we do?

Mr. MALCOLM. Well, as Senator Leahy pointed out in his opening statement, this is clearly a bipartisan issue and the number of investigations and prosecutions of child pornography and child exploitation cases has gone up each year for the past seven or 8 years, probably beyond that. In part, I am afraid it just shows the proliferation of this material as the Internet has literally exploded upon the scene.

Senator Congress has already done quite a bit to help us. The penalties for child molestation and child pornography offenses have dramatically increased with the PROTECT Act. We will have 25 new prosecutors devoted to this effort.

That having been said, this is a worldwide problem and a target-rich environment. A number of the perpetrators of these offenses are located overseas. Some countries cooperate with us more than others. I am not sure we will ever be able to really ever completely eradicate this problem.

Chairman HATCH. Would you suggest that we put out of business the networks that allow this to occur?

Mr. MALCOLM. I am sorry

Chairman HATCH. Do you suggest we put out of business the networks that allow this to occur?

Mr. MALCOLM. Well, of course, in order to do a criminal prosecution, you have to prove knowing involvement. As Mr. Morris, I believe, said, there are a lot of networks that may facilitate this activity by having a peer-to-peer system or allowing commercial websites. However, they don't always control the content that is out there and they don't necessarily patrol their systems. Certainly, one of the things that Congress can consider, which this Committee is considering, is regulating the means by which this material is propagated.

Chairman HATCH. Professor Jacobson, let me turn to you. I would like to discuss for a moment the circumvention practices in which the P2P networks engage which you talk about in your testimony.

It seems to me that when the computer owners choose to filter or block certain programs, that decision ought to be respected. The practices you identify, such as port-hopping, seem to significantly complicate the efforts of computer owners and system administrators to control what comes into their systems.

If we were to require that these networks and perhaps others on the Internet publicly register their ports and operate only through those registered ports, would that better enable computer owners to secure their computers against these unwanted materials?

Mr. JACOBSON. Yes. You would be able to filter out those protocols that you didn't want that matched those assigned port numbers. So that would allow an administrator as a first line of defense to better filter those things out.

Chairman HATCH. Mr. Morris, you insist in your testimony that the availability of child pornography on P2P networks pales in comparison to the quantity available on commercial websites on the Internet.

Even if true, do you not see a material difference between pornographic content, including child pornography, that is thrust upon juvenile P2P users whether they want it or not and websites to which access is granted only upon presentation of a credit card number usually available only to adult members of the household?

Mr. MORRIS. You make a differentiation, as indeed I did, between websites and peer-to-peer. I guess it is useful to go through what happens on peer-to-peer. When somebody does a search—and let's assume that they choose to take off the filter, willingly take the filter off—then they will search and they will get a list of search

terms. Those search also contain matter tags that describe what is in the file. So for somebody to download, they are going to have to click the file, watch it download, and then open it. So there are various processes. So the idea of files suddenly appearing doesn't really happen.

If, however, you look at the Internet, then you take those 40 million results. A lot of those sites you go to will be very sticky; they will stay on your computer. You can't close them. They will often download dialer applications that will send you on premium lines to Bermuda.

Senator LEAHY. Send you a what?

Mr. MORRIS. What they will do is they will download something called a dialer which will dial out of your computer—you guys know very much about this, yes—dial out of your computer to pornographic sites around the world, because their business is money. They sell pornographic images.

The other thing they will do is very often pop up. They use pop-ups, so they have teasers which are very explicit which will encourage the person to click on. The idea is then to lead them into either gratuitously pornographic sites, as the pedophiles do, or into then sites where they register a credit card. So the chance of somebody actually being exposed suddenly to a pornographic image is infinitely greater. Now, none of that says that because it is relatively small, it can be tolerated. But there is a significant difference between website and peer-to-peer.

Chairman HATCH. Mr. Hess, I realize the concerns that P2P networks raise in the university environment are not limited to, or even primarily stem from, the availability of pornography. We appreciate you coming here and enlightening us on the multiple challenges you face with respect to these networks.

You stated in your testimony that at times as much as 30 percent of the University of Utah's bandwidth is taken up with peer-to-peer file-sharing. Can you give us an estimate of what that costs the university?

Mr. HESS. If high levels of peer-to-peer were sustained throughout the year—it ebbs and flows depending on how many students are on campus—it could approach $1 million

Chairman HATCH. In your testimony, you mention the recording industry's recent pursuit of computer users making large numbers of copyrighted songs available on P2P systems. Do you feel that these types of actions are helpful or even necessary to get students to take copyright laws seriously?

Mr. HESS. Yes, at least that has been our experience on campus. Now the word is out that studets are being sued, it does make a difference, the amount of traffic has declined.

Chairman HATCH. In the last hearing, I suggested that with new technology they actually could blow up the computer after giving appropriate warnings.

[Laughter.]

Senator LEAHY. There was not uniform support on the Committee for that idea, I want you to know.

[Laughter.]

Senator LEAHY. We have joined on many of these things, but that is one where we kind of broke ranks.

Chairman HATCH. Only because of the lack of innovation on the part of those who didn't support it.

[Laughter.]

Chairman HATCH. But I think that more or less has awakened everybody to the fact that these are important issues, and it was one of the reasons why I did that. And I think it was very, very important to get out there that it is illegal what they are doing, that it is wrong, that if we don't have copyright, we are not going to have the creativity that this country is so noted for throughout the world.

This has been very, very interesting. I have a lot of other questions, but I am going to turn to the Democratic leader on the Committee and see what he wants to get into.

Senator LEAHY. Thank you, Mr. Chairman. I have found this a fascinating hearing. Unfortunately, because, as always happens on the Hill, you are supposed to be in three places at once, after these questions I will have to leave. I am going to have some that I will submit for the record.

I know, Mr. Spota, with a dozen of these fairly complex prosecutions you have brought recently, I am going to want to know more about that. That may well be a model for the rest of us. Of course, Mr. Callaway and I talk all the time on a number of these issues.

Mr. Morris, as you may know, the Internet service providers are required by Federal law to report all cases of child pornography to the National Center for Missing and Exploited Children. In fact, the statute states that the requirement is on anyone, quote, "engaged in providing electronic communications service or a remote computing service to the public through a facility or means of interstate or foreign commerce."

Now, under that definition, aren't you and other peer-to-peer networks covered by that statute?

Mr. MORRIS. I am not a lawyer and I wouldn't presume—

Senator LEAHY. What do your lawyers tell you?

Mr. MORRIS. That question as far as I know has never been asked. My interpretation as a layman would be very simple that in a technical sense it is not a network. What it is is a series of individual applications. Basically, as somebody said, it is like a net, a fisherman's net. So individuals sit there, there, and there, and they choose to share amongst each other. So I am very happy to ask our attorneys, but prime facie, I would suggest that, no, we are not covered.

Senator LEAHY. Well, let's talk about Kazaa. Would that mean that under this law they couldn't report pornography because they don't look at content?

Mr. MORRIS. Sorry. When you say "they," you mean we?

Senator LEAHY. Yes. Does that mean that you can't—

Mr. MORRIS. We technically—sorry to interrupt, Senator.

Senator LEAHY. Does that mean that you can't report pornography because you don't look at the content?

Mr. MORRIS. Precisely. There is no technical way at all. It is like asking Microsoft to look at the content of people's e-mails.

Senator LEAHY. You know, I would find that more believable, except that you find ways to find so-called spoofed files. Yes, you do.

Mr. MORRIS. Sorry.

Senator LEAHY. I will explain. If some of the companies and some of the artists who feel that their works are being stolen on your system and if they decide to put in a so-called spoofed file—that is, they have the name of an artist and the name of the record, but then they make sure that there is just white noise or something like that on it. Somebody would have to go through the whole downloading and do it. Somehow, you are able to check the content of that and those are taken off your network. You have ways of using filters to make it easy for children to circumvent those filters.

I mean, let's get real. On the things you don't want, the things that are going to cost you money—that is, having hundreds of white noise albums put in there—you can get rid of those. Why couldn't you get rid of the pornography, too?

Mr. MORRIS. I do not know any way that we can get rid of the spoofed files, or indeed the promotional files.

Senator LEAHY. But you do.

Mr. MORRIS. Sorry. Can you explain how, because I don't know?

Senator LEAHY. I have no idea. You are the ones who are running it. But, boy, they don't last on there very long. I think the next panel is going to point out that they have had artists that they represent try to put them on and then they don't last very long.

Mr. MORRIS. I understand what you are saying; the spoofed files, or indeed the promotional files that the record industry distributes very widely on KMD, and by their own admission.

We have something called an integrity rating. That is for users to self-clean. Now, users will indicate when a file is badly recorded. I mean, you must have come across a lot of files which are just poorly recorded. Similarly, users will tend to indicate that a certain file has a low integrity.

Now, we would certainly encourage users of KMD to use that mechanism to indicate when a file is pornographic. There is no specific category for pornographic; it is just low integrity. But if every user put pornographic files as low integrity—i.e. self-cleaning—then that would clean the network up very quickly.

So what you are talking about is the user community itself—that is not us at all—cleaning the network of files that they don't see as being of high integrity. I now understand what you are talking about. We have absolutely no control over that. Technically, we cannot.

Senator LEAHY. Well, you install on your users' computers software that tracks their activities online and puts advertisements on their hard drives based on what it shows. Are you also installing information on those computers about whether they are going to pornographic sites?

Mr. MORRIS. Sir, when you talk about installing applications—

Senator LEAHY. When your programs run, they also pick up information about the users so that you can run pop-up ads and do things like that. You don't do that?

Mr. MORRIS. No. Let me clarify for you.

Senator LEAHY. You have no way of tracking their activities online?

Mr. MORRIS. Absolutely none.

Senator LEAHY. None whatsoever?

Mr. MORRIS. There are some urban myths around that there is spyware or—

Senator LEAHY. How do you make money?

Mr. MORRIS. We make money through advertising. Let me clarify.

Senator LEAHY. Mr. Morris, I will let you finish. My time is running out here.

Mr. MORRIS. Sure.

Senator LEAHY. You make money by advertising, but you don't send the same advertising to everybody.

Mr. MORRIS. Precisely.

Senator LEAHY. If you have got somebody who consistently wants country and western, you are not going to be sending advertising for Beethoven's Third there. I mean, you and your advertisers just don't go out to everybody; they go selectively by how often the person is on. No?

Mr. MORRIS. No.

Senator LEAHY. So if somebody uses your system just once or if they use it 500 times, they get exactly the same ads?

Mr. MORRIS. Yes.

Senator LEAHY. They don't change?

Mr. MORRIS. Let me clarify. The side door application, which is similar to double click, which is the same sort of application that most of the major websites in the world use, serves the same ad. So a maximum of five pop-ups will be delivered in a 24-hour period. Those little banners you see—those are delivered to everybody.

Now, you may be talking about contextual advertising. Currently, we have no contextual advertising bundled with KMD; we have in the past. They have high levels of privacy and what they do—they are a separate applications and those applications are related to websites people visit. They are not applications we control and they certainly can't be used to track visits to illegal sites. I think that must be what you are talking about.

Senator LEAHY. Mr. Chairman, I will have some follow-up questions. I realize I have gone over my time, and I appreciate that I know there are other Senators who want to ask questions.

Chairman HATCH. Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman. I want to thank you for holding this hearing, and I thank you and Senator Leahy for spotlighting this issue. It is an issue important to parents like me, whose children's knowledge of computers and the Internet far outweigh my own. I am a big fan of the Internet and the amazing way it has improved our lives, from e-mail, to the World Wide Web, to the way it makes holiday shopping a breeze. We just drove my daughter to college in Boston and we got one of the fanciest hotels for $109 because we used the Web. I am not going to say what company right here, not at this table, Mr. Chairman.

But lately I have been concerned that this hallmark of the information age is getting bogged down. When you have such a new, major invention—I am sure this happened every time—there are all sorts of problems that emerge—spam, criminal activity in terms of fraud schemes.

And now comes news that the dark side of the Internet just got a little darker because of your excellent GAO report, Ms. Koontz,

which talks about how much child pornography has infiltrated the Web.

I am going to ask that my whole statement be read into the record.

Chairman HATCH. Without objection.

[The prepared statement of Senator Schumer appears as a submission for the record.]

Senator SCHUMER. But I do want to make one point, Mr. Chairman, and that is earlier today I was with D.A. Spota—and I want to commend you. Tom Spota is the D.A. of Suffolk County, one of the largest and most important counties in New York, and has done a great job as D.A. in general and on this issue, in particular.

Earlier today, he and I and Terry Schroeder, who is the President of ISAF, an organization that is dedicated to protecting children online, called on the Justice Department—or I called on the Justice Department to create a special task force to crack down on the traffic of child pornography by file-sharers. The task force would bring together the resources and expertise of the FBI and other Federal law enforcement agencies to find the best ways to track down and stop these criminals from peddling child pornography, and it would set up strong channels for information-sharing between the Federal task force and local officials like D.A. Spota to ensure that all levels of law enforcement are up to speed in this highly technical area.

In addition, Mr. Chairman, to strong law enforcement, I believe those in the technology industry need to step up to the plate. Those who profit from file-sharing technology have to do everything in their power to prevent the networks from being used for criminal activity, and that is where my questions will lead.

But first I wanted to ask D.A. Spota—as you know, I am asking for the creation of a national task force to focus on the challenges associated with the use of peer-to-peer networks to proliferate child pornography. The task force would bring together the several Federal agencies that deal with this problem and deal with the experiences of local law enforcement, like yourself, to ensure that all law enforcement is up to speed on the danger of peer-to-peer networks.

Do you think the task force is a good idea? Would it be helpful to local law enforcement, and are there lessons offices like yours could share that would be useful to Federal law enforcement?

Mr. SPOTA. Well, thank you, Senator. Certainly, it is a terrific idea. There is no question about that. I mentioned before in response to a question, I believe, by Senator Leahy or Senator Hatch that it seems to me that, as you say, a Federal task force is what is in order.

I am limited in our State jurisdiction. The Department of Justice and the U.S. Attorneys' offices obviously—their jurisdiction will extend throughout the United States, and I am sure even further, and I think that that is what is necessary.

Mr. Morris indicated to me before we were speaking—I may be wrong, but I think you might be located in Australia.

Mr. MORRIS. Mr. Chairman, if I may, we would be very happy to assist and advise that task force in any way we can. We are based in Australia. I am based in London. I have quite used to flying over. So we would be very happy to give you technical—

Senator SCHUMER. We don't want any of these meetings to occur in Hawaii.

Mr. MORRIS. There are some very nice islands in the South Pacific. But we would be happy, my chief technical officer or myself, to provide on a one-way basis, a one-way street, any information or help we could.

Senator SCHUMER. Great, thank you.

Well, thank you, D.A. Spota, and I appreciate your endorsement of this idea.

My next question is for Mr. Morris. As I mentioned in my statement, I think it is important that peer-to-peer networks do everything within their power to stop criminal activity involved in the sharing of child pornography through your software.

Your own terms of service agreement, which outlines the ways in which users are allowed to use the network and the license, suggests you will take measures to ensure that illegal or offensive content is not shared via your software, which is good. Your license agreement explicitly states in part that users, quote, "agree not to use the software to transmit or communicate any data that is unlawful, harmful, obscene, or otherwise objectionable," unquote.

Users who share child pornography files, including those charged in Suffolk County, violate this agreement and I want to know what you and your company are doing about it. What actions has Kazaa taken against these individuals in Suffolk County? Have you revoked their license agreement or sent them notices that they have violated the agreement?

Mr. MORRIS. Firstly, we do not know who the offenders are, but I am very happy to speak with you later.

A general point about the end user license agreement to which you refer. Yes, indeed, it does very strongly state that we can revoke the license. These, if you like, honor licenses are common throughout the Internet for downloading software. They are very much the questions you get asked in an airport, which say, you know, are you spy, do you have a bomb? The purpose of asking it is it does allow one, after the event, to do that.

Senator SCHUMER. This case got quite a bit of notoriety not just in New York, but around the country.

Mr. MORRIS. This is the first case that we have become aware of. If you care to tell me which users were actually using Kazaa as opposed to the hacks and the various other applications which you guys know sit on the fast-track network—perhaps if your colleagues could contact us—

Mr. SPOTA. They were all using Kazaa.

Mr. MORRIS. They were using Kazaa or Kazaa-lite?

Mr. SPOTA. I am sorry?

Mr. MORRIS. Were they using Kazaa-lite?

Mr. SPOTA. Oh, I don't know.

Mr. MORRIS. Yes. There are various clones and scamsters.

Mr. SPOTA. No, no. I hate to interrupt. For sure, they were using Kazaa, your company.

Mr. MORRIS. Okay. We would be very happy—in fact, as I said earlier, we applaud what has happened in Suffolk County because that sends a strong message to people that they are not anonymous

and that they will be found out. So, yes, we would be happy, if we had the address details, to serve such a notice.

Senator SCHUMER. Why hadn't you done it before this fortuitous meeting between you and Mr. Spota occurred?

Mr. MORRIS. Because technically it hadn't crossed my mind. I wasn't aware—

Senator SCHUMER. Would you in the future, on your own, if there are other cases like this or you hear that cases are being brought?

Mr. MORRIS. Surely. As I said earlier, I have only had contacts from four law enforcement agencies. As I said, in the early days of peer-to-peer, it was used on a pilot basis by pedophiles and they have tended not to use it in a systematic way since then because it is open and anonymous.

I would be very happy to work with the task force, and if any law enforcement agency does have details of specific users of KMD who have been prosecuted, yes, we would certainly send them such a notice.

Senator SCHUMER. A second question.

Chairman HATCH. Senator, your time is up.

Senator SCHUMER. Okay. I am going to try to ask some more questions on the next round.

Chairman HATCH. Well, we are going to submit written questions because I have got another panel and I have got to get through here.

Senator SCHUMER. Could I just ask one more, Mr. Chairman?

Chairman HATCH. Sure, go right ahead.

Senator SCHUMER. Thank you.

The next question is what kind of disclosure do you make to parents? In other words, would you consider letting them know that somehow or other, if their child uses Kazaa, they might be deluged, or at least be shown pornographic materials?

Mr. MORRIS. We are currently working with the industry association which has just been formed to find ways of doing that very thing. It is a two-stage process. Firstly, we support all measures to have parents actually understand what is on their kids' computers. That is the first stage.

Secondly, having done that, then make parents aware of the pitfalls of using the Internet, in general, and file-sharing programs in particular and where that might lead. So, yes, we are very happy to get behind those sorts of programs.

Chairman HATCH. I would like to see that happen because what we are dealing with here is pretty pathetic stuff, and your network basically is the network that is being used, Kazaa.

Senator Durbin.

Senator SCHUMER. Well, just—

Chairman HATCH. I hate to cut anybody off, but I do have to get through this hearing.

Senator DURBIN. I know you are trying, Mr. Chairman. Thank you.

Chairman HATCH. Yes, and we will keep the record open for questions because these are good questions my colleagues are asking, and I hope you will take the time to answer them.

Senator SCHUMER. I won't ask a question. I will just make a suggestion, and that is that Kazaa also try to give some funding to

ISAFE, which does the job pretty well. I would ask in writing that you respond to whether you would be willing to do that and to what extent. No answer is necessary.

Mr. MORRIS. We would be very happy to respond and I am virtually certain it will be in the positive.

Chairman HATCH. Senator Durbin.

Senator DURBIN. I would like to follow up on one question.

Mr. Morris, there was something you stated a little earlier that led me to believe this was the first time you had heard about this problem.

Mr. MORRIS. No, not about the—we have known that there is pornography and some instances of child pornography. When you say "this problem," you mean the general issue of—

Senator DURBIN. Your conversation with Mr. Spota, for example.

Mr. SPOTA. I think, sir, perhaps I misspoke. He was talking about the names of the people. That was our conversation.

Senator DURBIN. Well, Mr. Morris, if this has been a recurring problem or a chronic problem with your company, my question is this: Do the advertisers on your network ever ask you whether or not you have taken steps so that the network does not become a venue for this kind of child pornography?

Mr. MORRIS. I think the evidence from these data here show that it is not a chronic problem. Any single instance is a problem. As to whether advertisers have raised an issue, I don't believe they have, but I can check that out.

Senator DURBIN. That has frankly been a fairly effective way of changing policy in our country when those who are inadvertently or indirectly supporting this kind of activity come to know that their customers are not going to use their products. I would think that would be a concern to you from a revenue viewpoint, would it not?

Mr. MORRIS. It is a concern universally across the Internet.

Senator DURBIN. Mr. Spota, thank you for your leadership on this, but could you be more specific in terms of what you have found relative to his company and how it has provided access to this child pornography?

Mr. SPOTA. Well, what we found is basically contained in my testimony, but essentially children, in my view, are curious by nature. We all are, but especially children. I believe the people who are making this pornography and setting up these files are purposefully using terms that will be attractive to children—Brittany Spears, Pokemon, and anything with the word "young" in it.

I do disagree with Mr. Morris where he says, well, it is just by virtue of the fact that the file will obviously contain some pornographic literature. They will incorporate some term that will attract the attention of that child. So if a kid wants to look for something with "Brittany Spears," there will be a file name that will contain the name "Brittany," and oftentimes other names that have nothing to do with it. They will punch that on because of their natural curiosity. That is what is occurring.

Senator DURBIN. My other question to you is in terms of your prosecution, is it under State law that you are prosecuting?

Mr. SPOTA. Yes, it is, Senator.

Senator DURBIN. Do you find any limitations because you are dealing with State law in how far you can go by way of discovery or prosecution?

Mr. SPOTA. Absolutely, and that is why I am bound to prosecute only those who commit these crimes, possession or promoting child pornography, within the County of Suffolk. That is why I think it is so important that Congress act to give the Justice Department, the United States Attorney's Office, and the FBI the opportunity to prosecute these types of cases.

Senator DURBIN. Ms. Koontz, isn't that the GAO conclusion that there isn't clear delineation of Federal prosecuting standards? I think what I read in your GAO report is that we need more resources dedicated to this. Do you think the law is clear enough in terms of the prosecution?

Ms. KOONTZ. Actually, our study focused on identifying the level of resources that are devoted to peer-to-peer networks among the various law enforcement agencies. We were unable to determine how many resources were devoted because law enforcement agencies don't keep statistics in that kind of way. Our work has been much more focused on defining the parameters of the problem and I couldn't speak to the adequacy of the prosecuting standards.

Senator DURBIN. Well, maybe Mr. Malcolm can, because one of the concerns that I think we have is that since 2 years ago, there has been more and more focus of resources on terrorism. The FBI and other agencies have been told, frankly, drop some of your traditional activities or reduce your activity in them dramatically and move toward terrorism. That is our number one priority.

So what chance do we have here to have any kind of dedication of resources or aggressive effort involving the FBI when it comes to this problem of child pornography?

Mr. MALCOLM. Let me just say that in spite of this diversion of resources, the number of cases that we filed against child pornographers and child exploiters was up 22 percent last year. We don't work just with the FBI. We, of course, also work with ICE, we work with Postal, we work with various State and Federal agencies. We, in fact, work with the Internet Crimes Against Children Task Forces.

Let me stress that peer-to-peer is a serious problem. Don't get me wrong. Kazaa is only one peer-to-peer network, and in addition to that, there is a lot of this material out there on the Web. There is a lot of this material in chat rooms. There is a lot of this material in news groups. There are all kinds of emerging technologies that have presented ample opportunities for pedophiles to peddle their wares and to trade material and, through chat rooms, to contact kids.

Unfortunately, as I said before, this is a target-rich environment. Congress has already done a lot in terms of increasing the penalties through the PROTECT Act. You have given us additional resources. Unfortunately, this is such a worldwide problem that you are not never going to be able to eradicate it all. We are doing the best we can with what we have.

Senator DURBIN. Mr. Chairman, the last thing I will say on it is this. A few weeks ago, we had a family reunion and one of my nieces said that her son, a teenager in high school, didn't want to

come to the reunion because he just loves to stay on the Internet, she said. He is on there all the time. She went on to say, you know, I don't know a thing about it; I can't even tell you what he is doing there, but he just really loves it.

And I am thinking to myself, gosh, I hope that is going well. But that mother is in the same position many of us are who are not as conversant with the Internet as our children and grandchildren. So to say we are going to give the tools to parents many times is suggesting that they are going to develop a level of knowledge and sophistication about the Internet which is unrealistic. We have to develop other mechanisms to deal with this, and threats to those who would abuse it.

Thanks for this hearing, Mr. Chairman.

Chairman HATCH. Well, I want to compliment my colleagues for their questions, and also these comments. They are right on. You folks are in the forefront of this battle.

Mr. Morris, I know that you seem to be the person on target here, but there is good reason for it. I think unless you can help us to help you to get rid of this material, you are going to be under constant attack and ultimately we are going to have to do some things that would be very detrimental to your business. So I think you have really got to take this seriously.

Mr. MORRIS. Chairman Hatch, I think we do. I would say that I am willing to come over any time you want me to to work with you, your staffers, and anybody else here to help eradicate this issue.

Chairman HATCH. Well, we have had some good suggestions here today between you and Mr. Spota, and I think that could be true of other people as well. We appreciate your willingness to be able to do this, but it is serious stuff and we have got to do something.

The circumvention of security measures through various means such as port-hopping and the difficulties it raises have been brought to our attention through a number of different channels. I believe it is worth exploring what can be done to bring all these matters under control.

I know that Senator Leahy is going to work with me on this, as will other members of this Committee, and we will see what we can do to come up with some way of resolving some of these matters, or at least giving you the tools to be able to resolve them.

With that, I want to thank each of you for being here and we appreciate the efforts you have made and the information you have given us. It has been a very important hearing up to this point. So thank you very much.

Our second panel will address the ISP subpoena provisions of the Digital Millennium Copyright Act. This is a critical part of the compromise that this Committee helped negotiate between the content and the technology industries. This compromise was intended to permit both the development of Internet services and the enforcement of copyrights on the Internet.

If we could have order, I would appreciate it. Let's have order.

This compromise, which is now codified in Section 512 of the Copyright Act, creates so-called safe harbor provisions that protect Internet service providers from secondary liability for copyright infringement. These safe harbors protect ISPs regardless of whether

their systems act as conduits, locators, or hosts for infringing materials posted by third parties.

In exchange for these safe harbors, Section 512 requires ISPs to provide specific assistance to content creators alleging that someone is using ISP services or systems to host, locate, or transmit infringing content. For example, Section 512 can require an ISP to remove allegedly infringing materials hosted by the ISP, or to identify an allegedly infringing customer in response to a subpoena under Section 512(h) of the Act.

Recently, the subpoena provisions of Section 512(h) came under scrutiny when they were invoked by content creators trying to identify individuals allegedly trading infringing materials over peer-to-peer file-sharing networks.

Our second panel consists of three panelists who will discuss the legal and policy implications of the subpoena provisions that underlie both the Section 512 compromise and our broader system for reconciling copyright and the Internet.

Mr. Cary Sherman is the President of the Recording Industry Association of America. His organization has served Section 512(h) subpoenas to obtain identifying information about individuals alleged to have been trading infringing music files over peer-to-peer file-sharing networks.

Mr. William Barr is the former Attorney General of the United States and is the General Counsel of Verizon. His company provides ISP services and has received Section 512(h) subpoena.

Our last panelist, Ms. Marybeth Peters, if the Register of Copyrights. She brings to this narrow but important dispute about Section 512(h) subpoenas her unquestioned expertise with the broader issues of law and policy that underlie both the DMCA and the Copyright Act. She has also been gracious enough to help us streamline this large hearing by agreeing to appear on the same panel as our private-party witnesses and agreeing to go last in order to provide some perspective on the views of the two preceding folks.

I just want to express my gratitude for having all three of you here. All three of you are leaders in the respective areas in this field, and we are just very grateful to have you here.

I think we will start with you, Mr. Sherman, and then we will go to General Barr and then we will come to Marybeth.

STATEMENT OF CARY SHERMAN, PRESIDENT AND GENERAL COUNSEL, RECORDING INDUSTRY ASSOCIATION OF AMERICA, WASHINGTON, D.C.

Mr. SHERMAN. Thank you, Chairman Hatch, for inviting me to testify today and for your ongoing commitment to protecting intellectual property. We are all very grateful.

My name is Cary Sherman. I am the President of the Recording Industry Association of America, the trade association representing the U.S. recording industry. Our members create, manufacture, and/or distribute 90 percent of all legitimate sound recordings in the United States.

I would like to take just a minute up front to give the Committee some information regarding some announcements we made yesterday. Following a multi-year campaign to educate the public about

the illegality of unauthorized downloading and the launch of more than a dozen high-quality, low-cost, legitimate online music services, the RIAA filed lawsuits yesterday against more than 250 individuals who were sharing, on average, over 1,000 copyrighted music files on public P2P networks.

We simultaneously announced a program to grant what amounts to amnesty for individuals who voluntarily identify themselves and pledge to stop illegally sharing music on the Internet. Should you have any questions about it, I would be pleased to respond to them later.

We would have preferred to avoid litigation, but we could no longer simply stand by and watch while our products are stolen in mass quantities and the livelihood of thousands of artists, musicians, songwriters, recording companies, and retailers are destroyed. We hope that this ongoing effort will educate the public about the consequences of online piracy and help foster an environment in which a legitimate online music marketplace can thrive.

Let me now turn my attention to the topic of today's hearing. Let me just begin with some startling statistics. Over the past 3 years, shipments of recorded music in the United States have fallen by an astounding 31 percent. Hit records have been impacted most dramatically.

In 2000, the top 10 selling albums in the U.S. sold a total of 60 million units. In 2001, that number dropped to 40 million, and last year it totaled just 34 million. The root cause for this drastic decline in record sales is the astronomical rate of music piracy on the Internet.

Although there is no easy solution to the piracy problem, one thing is clear. Verizon's DSL subscribership is growing due to the explosion in the use of P2P, and it is very troubling to our industry that Verizon actually encourages its new subscribers to visit unauthorized P2P services instead of legitimate licensed sites as their preferred source for music online.

If you sign up for Verizon DSL, you get a brochure, "Your Guide to Broadband Living and Content," that tells users, and I quote, "Subscription sites do offer up MP3s to download. However, they typically don't offer music that is selling exceedingly well in stores. By contrast, the free sites are likely to have pretty much everything, but you may get pelted with some unwanted ads." And people wonder why the copyright community is skeptical of Verizon's claim that the real issue is privacy and not piracy by their subscribers.

After all, nowhere in the brochure does Verizon warn its customers about the serious privacy threats of using P2P. Think about it. Kazaa has been downloaded over 250 million times, and many of those who use it are unwittingly sharing sensitive personal information—e-mails, tax returns, financial and medical records—with millions of others on the Internet. You would think that a company as concerned about privacy as Verizon claims to be would warn its subscribers that they are committing privacy suicide when they put Kazaa on their computers.

So what does all of this have to do with what we are talking about today? First, it helps explain why RIAA's members, with the support of a broad array of other organizations in the music indus-

try representing artists, songwriters, music publishers, and others, took the action we announced yesterday, and why Judge Bates conclusively decided on two separate occasions that the DMCA information subpoena process does apply in the P2P context and that the real privacy threat is millions of users essentially opening their computers to the world.

Second, and perhaps most important for this hearing, they illustrate that Congress, under the leadership of this Committee, saw the future in 1998 when it passed the DMCA. The rampant piracy of music on the Internet is a true-to-life example of exactly the kind of problem Congress envisioned copyright owners would face in the digital world.

Although P2P technology did not exist in 1998, Congress understood that the Internet and advances in technology would lead to an explosion in online theft of intellectual property. So in exchange for exempting ISPs from any liability for the infringing activities occurring on or over their networks and connections, subject, of course, to certain prerequisites, Congress created a framework by which copyright owners, with the assistance of ISPs, could expeditiously identify individuals engaging in infringing activities online. That compromise—expeditious access for copyright owners to identifying information of infringers in exchange for broad liability limitations of ISPs—is as fair today as it was in 1998.

Five years after the passage of the DMCA, we hear nothing from Verizon about changing its liability limitation, but a lot about its concerns over privacy. I just want to mention one thing. No one has a privacy right to engage in copyright infringement on the Internet, and illegally sharing or downloading copyrighted music online is not a form of free speech or civil disobedience protected by the First Amendment.

As I understand Verizon's privacy argument, disclosing its subscribers' identifying information pursuant to a valid DMCA information subpoena threatens to violate its subscribers' privacy because the information subpoena process, in their estimation, is susceptible to abuse and does not provide the same protections afforded by a more traditional John Doe lawsuit.

But Congress considered and decided this question back in 1998. Ironically, the very principle ISPs profess to defend, the privacy of their subscribers, is at greater risk in a John Doe action than through the information subpoena provisions of the DMCA. There are statutory limits on the type of information a copyright owner can obtain via an information subpoena and the purpose for which that information can be used.

A copyright owner can only receive information that is necessary to identify and contact the alleged infringer. More importantly, the copyright owner is statutorily limited to using that information exclusively for purposes of enforcing their copyright.

Compare that to the John Doe alternative where a copyright owner can request anything related to the ISP subscriber account, including user habits, website visits, payment records. And once that information is provided to a copyright owner, there are no statutory restrictions whatsoever on how it can be used or with whom it can be shared.

RIAA and the copyright community as a whole are committed to protecting the privacy of individuals and support the balance that was struck by this Committee and the Congress in the DMCA to protect both privacy and ensure the enforcement of copyrights.

Congress anticipated the needs of copyright owners and the rights of individuals in the DMCA, and enacted a provision that has been upheld and validated by the courts and constitutional scholars. As the content community continues to face the challenges of digital piracy, Congress must ensure that tools are available to limit costly damages in an expeditious manner. Our Nation's cultural assets, balance of trade, and world leadership in intellectual property depend on it.

Thank you very much.

[The prepared statement of Mr. Sherman appears as a submission for the record.]

Chairman HATCH. Well, thank you.

General Barr, we will turn to you.

STATEMENT OF WILLIAM BARR, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, VERIZON COMMUNICATIONS, WASHINGTON, D.C.

Mr. BARR. Thank you, Mr. Chairman, Senator Durbin.

We believe that the health and the vitality of the Internet as a medium of communications in our society depends on the availability of a rich array of content, which in turn requires vigorous protection of intellectual property rights. But at the same time, we think it also depends on the public's confidence in the privacy and security of the Internet as a communications medium and their assurance that there is some protection for private information.

Our concern is that a very ill-conceived blunderbuss approach to addressing the first set of issues, intellectual property, is being applied in a way that is riding roughshod and ultimately sacrificing very real privacy and safety concerns.

Now, from the opening statement of Mr. Sherman it would appear that Verizon stands alone in this, when, in fact, as the Committee is aware, there are 92 groups supporting our position, including library associations, civil liberties groups, child safety groups, and numerous other Internet service providers.

Mr. Sherman sort of suggests that our interest in privacy is somehow this new-found interest and is not really altruism here; it is economic interest. Well, be that as it may, our point in our opening statement is that privacy is important to the well-being of the Internet, just as important as intellectual property rights, the ability of individuals to know that their private information is not going to be handed away willy-nilly to other people.

Now, I think what is going on here is that the RIAA is taking the subpoena provisions of the DMCA and radically expanding them to apply to an area that they were not intended to apply to. That is our view. This sweeping subpoena that they claim, bereft of any of the safeguards that have been employed throughout our history to protect privacy concerns and place checks on the availability of private information, poses, we think, a threat to personal privacy and First Amendment rights.

We further think that the tactic of using these massive subpoenas has really sidetracked the recording industry into this inter orem campaign against 12-year-old girls rather than pursue collaboratively with the network industry a long-term, effective technological solution, as Congress explicitly envisioned in the Act, working collaboratively to develop a long-term technological solution to this problem.

Our view is that both the take-down provisions and the subpoena provisions in the Act were expressly directed at infringers who were storing material on service providers' facilities. So they were distributed copyrighted material from websites that were hosted on the internet service providers' facilities.

We believe the subpoena provisions were meant to allow for the identification of the individuals who were storing that information on the facilities of the Internet service providers. Indeed, our view is that the subpoena provisions explicitly cross-reference the provisions dealing with the storage of information three times.

Now, in that context, there are some safeguards for these privacy concerns because we have control and access to that information. It is right there on our system, and when we are served with a subpoena, we can immediately verify whether there is a legitimate basis for the property owner's concerns. Further, the privacy concerns are somewhat diminished because the party has voluntarily given this information to us to store. Indeed, other provisions of the Act, sections (f) and (g), provide protections to owners who have done that.

Our view is that the subpoena provisions were never intended to allow private parties unfettered power to delve into what individuals have on their own desktop or laptop hard drives, or into the nature of direct communications from one computer to another.

The RIAA is claiming a radical new process—it is heretofore unknown in the law; the district court acknowledged it was a novelty—to obtain personal and private information about electronic communications without the safeguards that have always been applied even to government investigations or in civil lawsuits, and without any accountability for how that information is used.

The process goes like this. When people are using the Internet, they can generally rely on some protection of their identity. When they are browsing or in chat rooms or sending e-mails, the computer does reveal a number, the IP address, which cannot be correlated to an individual.

But under RIAA's interpretation of the Act, any individual can simply fill out a one-page form. They can assert that they have a copyright interest. It doesn't have to be a registered one that would serve as the basis of a lawsuit, and Federal copyright protections cover a broad array of any expressive activity—pictures, content of e-mails, and so forth.

Then they can assert a good-faith belief that their copyright interest is being infringed, and that is the basis upon which they can compel the surrendering of any individual's name, address, telephone number. And now they claim they can get the e-mail address of any Internet user. Not only do they get that identification information, but they are able to correlate it to specific communicative activity on the Internet, to those individuals.

This is not done in connection with a pending lawsuit or a grand jury investigation. There is no judicial supervision of this. Nobody looks at this at the courthouse. It is just served on us and we have to comply. No one reviews the bona fides of the requester. No one reviews whether there is, in fact, copyright information involved. No one determines whether, in fact, there is a reasonable basis for the allegation.

Unlike the information that the government is supplied in an investigation, there are no express safeguards provided for this information and how it is used. There is no requirement to file a civil lawsuit. There are no express sanctions or penalties for the misuse of this information or for its disclosure into the public. There are countless illicit ways that this information can be used without the victim every knowing, without anyone ever knowing how it came to be that their identity was disclosed and exploited in some way.

This goes far beyond the power that this Congress gives Federal investigative agencies who are investigating things like pornography, who are investigating things like terrorism. The Government doesn't have this power.

This is very analogous, for example, to pen registers and to trap-and-trace. The Government just can't go and fill out a one-page form and claim a belief that it would be helpful. They have to have a judge review it and a judicial order based on a certification that it is relevant to an ongoing investigation, and that material is under seal. So when the Government acts in an investigative capacity, this Congress, consistent with constitutional liberties, has ensured that there are safeguards. But given the sweeping nature of this power, deputizing commercially-interested individuals to go out and do this kind of thing, abuses aren't just possible, but abuses are inevitable.

This is not just a tool that is going to be used by legitimate groups like RIAA. This is a tool that can be and is now being used by pornographers themselves. It can be used by pedophiles and stalkers.

Think about the pornographers. We have already had a case since the district court decision where a group that makes gay pornography has sought the names of 59 individuals who they claim were exchanging this pornographic material. And now they have announced, as RIAA has, their own amnesty program. Do you know what the deal is? If you buy our hard-core pornography, we won't come after you. Just think of all the abuses that pornographers can use. People visit a website, they get the IP address, and they can blackmail those individuals.

Now, think of stalkers. There is nothing in here that requires a stalker to give his real name, or a pedophile. They meet someone in a chat room, go down to their local district courthouse, fill out the form, use a false name, and we have to surrender the information, the identity of these people. That is an outrage. That doesn't exist in any other context in the law and it has to be stopped.

Even where there are legitimate interests, such as RIAA's interest, the blunderbuss power that they are applying here inevitably is going to result in mistakes and abuses, and it already has. There is now a sub-industry of bounty hunters that goes about hunting down people. Congress is many times worried about bounty hunt-

ers when they are involved in law enforcement activities, but now we have commercially-interested bounty hunters who can go and get these documents.

We have robots like in "Minority Report," you know, spiders crawling around the Internet with little lights on their foreheads looking for files. That is all very fine, except they find a book report, which they did, a kid's 1-kilobit book report on Harry Potter, and they get slammed by the RIAA. Just recently, they tried to shut down the computers of, I think it was Penn State astronomy department because it found the name Usher in a file; obviously, in their mind, some kind of recording artist, but, in fact, the name of the department head.

So this is the kind of force that has been loosed onto the Internet, and our position is if this is what Congress wanted, it is a disgrace and it should be stopped. If this is not what Congress, if this was not the intent of the legislation, then Congress should act now and deal with it, and not wait for years of litigation and this kind of activity to bring a terror campaign against individuals without any kind of due process.

Congress did spell out how it thought, and rightly so, in my view, this was to be addressed in Title I of the legislation, which is technological protection for the content. The content can be wrapped. It can be protected through encryption, it can be protected through access code protection. Working collaboratively with the networks, that can be pretty much immune from attack and defeat. In fact, Congress has passed laws in Title I saying it would be a crime to try to circumvent those kinds of protections once we worked them out.

But ever since they have embarked on this cat-and-mouse game with teenagers, they have had no interest in coming to the table and talking about this long-term technological problem, which means what? Which means you are going to have a technological arms race with efforts to evade this and hide IP addresses and all this cat-and-mouse stuff going on, instead of something that Congress has already laid the ground work for, which is a regime of protecting content, of having the networks and the content providers work to develop a scheme, and has already passed a law saying it is criminal to try to evade that scheme. So this is largely a wasteful, self-defeating effort.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Barr appears as a submission for the record.]

Chairman HATCH. Well, thank you. We are going to need to have you give us your best ideas as to how to resolve some of these problems that you have raised.

Ms. Peters, we will turn to you.

STATEMENT OF MARYBETH PETERS, REGISTER OF COPYRIGHTS, U.S. COPYRIGHT OFFICE, WASHINGTON, D.C.

Ms. PETERS. Mr. Chairman, Senator Durbin, I am pleased to testify at this very timely hearing. Senator Hatch, you were among the leaders in drafting and enacting the Digital Millennium Copyright Act, and I know that these—

Chairman HATCH. You would have to say that after General Barr's comments.

[Laughter.]

Ms. PETERS. I am going to say it is a good thing.

Mr. BARR. Properly interpreted, it is a good thing.

Chairman HATCH. Excuse me to interrupt again. We need both of your ideas on how we solve these problems because much of what he says I agree with; in fact, most everything. Yet, I see where you are right, too. In other words, RIAA should not have to put up with the wholesale pilfering of your copyright materials. So we need to have some help here and maybe if you two could get together and give us some advice, it would be very helpful because this is important stuff.

Then, Ms. Peters, of course, we are going to rely on you to help us, too. Go ahead. I am sorry to interrupt you.

Ms. PETERS. What I was going to say is that I know these issues are important to you, as they are to me.

In 1999, Napster popularized peer-to-peer technology and tried to turn it into a profit-making business. In a remarkably short period of time, Napster was being used by millions to copy and distribute an unprecedented amount of copyrighted music.

We agreed with the Ninth Circuit's holding that Napster users infringed at least two of the copyright-holder's exclusive rights—reproduction and distribution. Since Napster's departure, other businesses utilizing peer-to-peer technology, such as Aimster, Grokster, and Kazaa, have appeared.

Mr. Chairman, make no mistake, the law is unambiguous. Using peer-to-peer networks to copy or distribute copyrighted works without permission is infringement, and copyright owners have every right to invoke the power of the courts to combat such activity. Every court that has addressed the issue agrees.

Copyright law has long recognized that those who aid and abet copyright infringement are no less culpable than direct infringers themselves. Based on this principle, the Ninth Circuit Court correctly found that Napster was both vicariously liable and a contributory infringer. Unfortunately, the *Napster* decision was not the last word on the matter.

Earlier this year, a Federal court in California surprised many when it held that *Grokster* and Streamcast are not liable as secondary copyright infringers. Mr. Chairman, these are people whose businesses are dependent upon massive copyright infringement. Any application of the law that allows them to escape liability for lack of knowledge of those same infringements is inherently flawed.

The *Grokster* decision was wrongly decided, and if it is upheld, it will be a major impediment to the fight against massive online infringement that is so rampant today. *Grokster* is not the last word on the subject, either. The decision in *Aimster* is reassuring.

Hanging over all of these cases, however, is the Supreme Court's decision in *Sony*. The correct application of the doctrines of secondary liability in the *Sony* case should produce findings of liability for the proprietors of *Grokster*. If that is not the result, *Sony* should be revisited by the Supreme Court or by Congress.

Unless and until the *Grokster* decision is overruled, copyright owners have no choice but to pursue the individual peer-to-peer

users who are actually engaging in infringement. While copyright owners have expressed regret that they are compelled to take this step, they need offer no apology. People who use peer-to-peer technology for unauthorized reproduction or distribution of copyrighted works are breaking the law.

Litigation and even publicity about the subpoenas have made clear to everyone that the so-called file-sharing of copyrighted works is not an innocent activity without legal consequences. Knowledge that such conduct may lead to expensive and burdensome litigation and a potentially large judgment should have a deterrent effect.

Copyright owners have every right to enforce their rights in court, whether they are taking action against providers of peer-to-peer services designed to profit from copyright infringement or against persons engaging in individual acts of infringement.

To take action against users of peer-to-peer networks, copyright owners must know who those users are. Congress recognized this and included in the DMCA a process by which owners can learn basic identifying information about alleged infringers from their Internet service providers.

As you recall, the DMCA began as an effort to implement the 1996 WIPO Internet treaties. However, as this legislation moved forward, ISPs demanded that it include limitations on their liability for copyright infringements carried out over their networks. Congress heeded this call and provided the ISPs with a huge benefit: virtually no liability for qualifying ISPs.

This was balanced by placing on ISPs certain obligations. One requires ISPs to respond expeditiously to subpoenas seeking identifying information about subscribers accused of copyright infringement. The ability of copyright owners to use Section 512(h) is a critical part of that bargain, allowing copyright owners to pursue primary infringers.

Recently, the scope and constitutionality of Section 512(h) has come under attack. In the RIAA–Verizon litigation, Verizon claims that the subpoena power of 512(h) is inapplicable to the mere conduit activity described in 512(a).

As the district court held, the plain language of 512(h) demonstrates that this interpretation is not correct. I agree. The statutory text confirms the compromise that copyright owners and ISPs are to work together to remedy infringement in all categories of activities.

The United States has intervened in the Verizon litigation to defend the constitutionality of Section 512(h). The Copyright Office has assisted the Justice Department in this effort and we firmly believe that 512(h) is appropriate and constitutional.

One observation. The alleged constitutional infirmities apply to any subpoena applied pursuant to 512(h), not only to subpoenas to identify participants in peer-to-peer networks. And if 512(h) is declared unconstitutional, I believe the result would be that 512 as a whole, including the limitations on ISP liability, would be unconstitutional.

In conclusion, the DMCA represents a carefully crafted and balanced bargain which utilizes both enlightened self-interest and the incentives created by doctrines such as secondary liability to en-

courage all stakeholders to work together. Some are now selectively challenging key components of that bargain, particularly in the context of peer-to-peer technology.

Taken together, the positions of Grokster along with arguments now made by Verizon and others, if they prevail, will leave copyright owners with little or no remedy against the most widespread phenomenon of infringement in the history of this country.

Thank you.

[The prepared statement of Ms. Peters appears as a submission for the record.]

Chairman HATCH. Well, thank you. You answered one of my major questions there. Let me just say before I turn to Senator Durbin, who will be our last questioner, I want to thank the members of this panel for your testimony.

I think that these issues have not ripened enough to permit this Committee to determine whether Section 512(h) works as intended or whether legislation could be brought to improve it. The first court challenges to 512(h) subpoenas are still ongoing and I don't think we can yet determine whether these subpoenas are being used responsibly to identify alleged infringers. More actual experience with these provisions could reveal potential improvements to them.

Perhaps in the meantime, what I would like to do over the next 6 months is I would like to ask Verizon and the 92 companies that are supporting your position, General Barr, and RIAA and any affected consumers to report back to me and my staff and Senator Leahy and his staff at least bi-monthly on how the subpoenas are operating and how further legislation might improve them.

In these reports, I would ask both of you to keep two principles in mind. First, the Section 512(h) subpoena process exists because ISPs, as Ms. Peters made clear, argued successfully and over the objections of the content creators that they should be immune from secondary infringement liability because individuals misusing ISP services were the proper targets for Internet copyright infringement.

This broad immunity ensured, as Ms. Peters said, that only viable targets for copyright enforcement would be individual Internet users who guessed wrong about whether Internet content respects the complex strictures of copyright.

The interests of those burdened consumers, it seems to me, are critically important. But a claim that their interests cannot be reconciled with content creators' need for efficient identification mechanisms seems like a claim that the intent of Section 512 cannot be achieved without the reopening of all of Section 512. That is not a claim that should be made or accepted lightly.

Secondly, the Committee needs statistically valid data to support any claims about consumer preferences. Copyright-holders have long used means short of Federal lawsuits to resolve disputes with alleged infringers. Valid data would help this Committee determine whether individual Internet users actually prefer a mechanism that requires them to be identified not as the private recipients of cease and desist letters, but as named defendants in public Federal court complaints seeking damages, statutory damage fees, and injunctions.

So what I am hoping, Mr. Sherman and General Barr, is that your organizations will help us here and provide this Committee with—I would like bi-monthly reports and proposals that I have requested. Now, that is a little work, but my goal here is not to find fault with either of you. I think both of you make good cases here. It is try and get this system so it really does work, work efficiently, work constitutionally in a sound manner, and work to the betterment of copyright protection.

It is complex. I mean, it took us 5 years to get the DMCA passed, and I can remember all of the back and forth, absolute gut fights that we were in to get that done. I have no doubt that it is not perfect. On the other hand, I think we might be able to resolve some of these problems in a way that would be mutually beneficial and perhaps satisfactory.

Naturally, content providers and copyright owners have a tremendous interest in their protection. Naturally, service providers have a different set of interests, as well as those interests, and we need some help here as to how best to solve these problems.

I think these young kids or anyone else wouldn't think of walking into a record store and stealing CDs right off the shelf, and yet that is exactly what they are doing over the Internet. And that is just one aspect of it. There are movies, books, CDs, you name it, and we have got to find some way to have our society be honest about these very important copyright protections. So if I could get some help from both of you, I would appreciate it and I will count on it.

Senator Durbin, you are going to be our last and then I have got to close up shop here.

Senator DURBIN. Thanks, Mr. Chairman. I am going to be brief here.

Mr. Barr, I thought you made a pretty compelling argument, but I am really troubled by this brochure if it accurately depicts what you were advising your customers to do, which is to use the free sites, the P2P sites, for acquiring music. It strikes me that you don't come to this discussion with clean hands.

Mr. BARR. Senator—

Senator DURBIN. If I can finish, it strikes me that you are encouraging them to use these sites which basically open up their privacy to the world, and I think Judge Bates made that observation when he said that this peer-to-peer file-sharing, as quoted by Mr. Sherman, "It is hard to understand just what privacy expectation a user has after essentially opening his computer to the world."

It strikes me that it sounds like you are encouraging Lady Godiva to get on the horse and then complaining that the arresting sheriff is sneaking a peek and invading her privacy. I mean, I don't think you can have it both ways.

Mr. BARR. Well, Senator, if you have the brochure in front of you, you will see that the very first paragraph of the brochure says that the courts have ruled that groups like Napster and that kind of sharing is a violation of law, and that it is quite possible to get your needs satisfied on the Internet with a completely clean conscience. That is the first paragraph.

The paragraph that Mr. Sherman quoted from, after elision—you will note that that paragraph starts off by listing a number of sites,

like Rhapsody and MP3, and so forth, and then makes the distinction between subscription sites and free sites. Now, free sites can be authorized sites. Free sites is not a synonym for P2P.

So that paragraph was intended to list the lawful, authorized sites, some of which are subscription, some of which are free, and then explain the difference between subscription and free sites.

Senator DURBIN. So, Mr. Sherman, are you misrepresenting this by saying that this quote and the one that you have highlighted here are an invitation to P2P and an invitation to squander your privacy?

Mr. SHERMAN. No. I stand by my quotation. I will admit that the 2003 version is an improvement over the 2002, which specifically proposed people to go to the Morpheus site, which is one of the illegal sites that we have had the most problems with. So Verizon has improved it a little bit.

Just when you look at "the free sites have pretty much everything you want, but you may be pelted with some unwanted ads," how about the fact that you may also be engaging in illegal activity about which the recording industry announced 6 months ago that we intend to bring lawsuits to enforce our rights? That would be a service to the DSL subscribers, not the sort of notice that is being given here.

Senator DURBIN. Let me ask you about what was announced yesterday by your industry. Are you headed to junior high schools to round up the usual suspects? How are you going to deal with this in a fashion that doesn't turn off your potential customers for a long time to come?

Mr. SHERMAN. Well, the word "customers" is an interesting term because if somebody doesn't actually buy your product but simply steals it, what do you consider them? What is the shoplifter at Saks Fifth Avenue? Is that a customer?

Senator DURBIN. So you write them off?

Mr. SHERMAN. Well, no, we don't write them off. We try to bring them back, and we try to bring them back by letting them know that this is really illegal activity, that they are not anonymous when they engage in it, and that there can be consequences.

We have done a lot of market research and we have come to the unhappy conclusion that people don't shoplift not because it is immoral or because it is wrong, but because they fear they may get caught. And we are trying to let people know they may get caught, and therefore they should not engage in this behavior.

Yes, there are going to be some kids caught in this, although you would be surprised how many adults are engaged in this activity. This is not just children. But we think that it is great for parents to know what their kids are up to. If a child brought home a shoplifted CD from Tower, I don't think the average parent would say, oh, look how cute, he loves music. They would make him take that CD back and lecture him about honesty and theft, and so on and so forth.

Parents need to know what their kids are doing when they are downloading music from the Internet, too, as well as everything else we have talked about at this hearing today—the access to pornography whether they want it or not, the child pornography, the security threat, the privacy threat.

Parents may not realize that their kids are opening up the parents' hard drive for the rest of the world to see. That would be a service if ISPs notified their customers that there is a privacy risk to engaging in illegal file-sharing activity on these peer-to-peer networks.

Senator DURBIN. I think that is a very constructive suggestion, and I don't mean to downplay the threat to your industry when I suggested that you are going after adolescents. I think it is a serious problem. It is theft and it should be viewed as such. I think you have a tough public relations campaign here to go after the offenders without appearing too heavy-handed in the process.

I would say, Mr. Barr, that we have found, I think, in both political parties that privacy is one of the most important things that Americans want to protect, whether it is medical privacy or financial privacy. I think we are learning. Senator Hatch and I—and I respect his leadership on this—are learning and hoping that we can make the laws that we have passed better in the future.

I thank you all for coming to this hearing. Thank you, Mr. Chairman.

Chairman HATCH. Well, I appreciate your kind comments. I have to say that nobody respects privacy rights better than I do, and I understand all of the concomitant liabilities you would have if those privacy rights are not respected. There are all kinds of problems that would come forth.

All three of you have been terrific. I think we have benefitted a great deal from this, and I agree with you that, yes, there are some children doing this, but there are a lot of adults doing it as well, who ought to know better and who deliberately do it knowing that it is wrong. It is just time for people to wake up.

I would hate to get to that point where we have to give three warnings and then blow up the set. I am speaking tongue-in-cheek to a large degree, but there is still a lot of truth to that, and I have to say that this hearing has been very beneficial.

Ms. Peters, I have always respected you. I think you are one of the best servants in Government that we have, and we appreciate your viewpoint here today. It was well put and something I am extremely interested in, and we appreciate the efforts that you have put forward. Help us to be able to do a better job to be able to protect the respective interests and to resolve some of these difficulties.

I have no ax to grind here. I just want to make sure that we resolve these difficulties that exist and that we live within the framework of laws. To that degree, I think you folks can be of tremendous help to us. So with that, I want to thank you again.

Let me just make one more comment. The deadline for submitting written questions to witnesses will be 5:00 p.m. next Tuesday, September 16. So I hope all staff will pay attention to that.

Thanks so much, and we will recess until further notice.

[Whereupon, at 4:33 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

Response to Questions from Senate Judiciary Committee

Questions from Senator Chambliss

Q1. Mr. Barr, what is the impact on service providers in terms of responding to the hundreds of subpoenas you have received?

A1. The hundreds of subpoenas discussed in my testimony had been issued under 17 U.S.C. § 512(h), which creates a procedure for the issuance of subpoenas addressed to online service providers without judicial supervision in certain circumstances. Copyright owners had been using section 512(h) to issue subpoenas against peer-to-peer file sharing, which Verizon did not believe was an authorized, or appropriate, use of the special section 512(h) subpoena process. On December 19, 2003, the US Court of Appeals for the District of Columbia Circuit agreed with Verizon and held unanimously that Section 512(h) does not apply to online service providers when they are acting as a conduit for online traffic. Rather, the Court held that section 512(h) only applied where content was stored on a service provider's servers. *RIAA v. Verizon Internet Services, Inc.*, 351 F.3d. 1229 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004). The Eighth Circuit agreed, shortly thereafter. *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771 (8th Cir. 2004). To a large extent, the impact on service providers is now moot. Since the Court of Appeals' decision, RIAA has been obtaining court-ordered subpoenas on a regular basis and sending them to Verizon pursuant to a process both parties have found acceptable. Verizon has promptly responded to the subpoenas and as distributor of content, believes strongly in copyright protections and compliance with copyright enforcement in partnership with the content community.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.001

Q2. Mr. Barr, you have stated that the subpoena process under the Digital Millennium Copyright Act is less protective of parties' interests than is true of the traditional subpoena process. How is this so? Can you compare the process law enforcement must go through with the process the Recording Industry Association of America is using to get identifying information?

A2. After the Court of Appeals' decision, content owners, including the RIAA, began filing John Doe lawsuits and obtaining traditional subpoenas issued with the appropriate judicial oversight The traditional subpoena requires that the copyright owner file a valid complaint in federal court, investigate the facts and inquire into defenses and prove ownership of a federal copyright registration. Under the traditional subpoena process, defendants also enjoy fundamental due process protections, including notice, the opportunity to be heard and to raise defenses. Judicial oversight deters potential abuses as does the availability of FRCP Rule 11 sanctions. None of these protections were part of the old RIAA form subpoena process. Similarly, government entities under a variety of criminal statutes, including the Video Privacy Protection Act and Cable Communications Policy Act, can only obtain subscriber information subject to extensive limitations and pursuant to court order or judicial supervision. This issue, however, is now largely moot. In the preceding five years, the filing of John Doe lawsuits has not interfered with copyright owners' enforcement activities. As RIAA President Cary Sherman stated in a press release shortly after the D.C. Circuit's 2003 decision, "[o]ur campaign against illegal file sharers is not missing a beat." He confirmed that "[t]he 'John Doe' legal process is a well-established mechanism for aggrieved parties to enforce their rights. The process by which we obtain the identity of defendants has changed, but the enforcement program has not." *See* http://www.riaa.com/newsitem.php?news_month_filter=1&news_year_filter=2004&resultpage=&id=7A2318DB-1A51-7911-AB93-54D8337A9B90.

Question from Senator Cornyn

Q. The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would it even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997) be amended, so that any reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. § 506(a)(2)?

A. The thrust of the question appears to focus on whether a consumer's infringing conduct should be subject to enhanced criminal liability with respect to pre-release materials. It is our understanding that Congress addressed this issue in Title I of the Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9 (enhancing criminal penalties for infringement of works "being prepared for commercial distribution" including by "making it available on a computer network").

On the broader question related to the fair use doctrine, the Copyright Act expressly recognizes that "the fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of [the four fair use factors]." 17 U.S.C. § 107. In *Harper & Row, Publishers v. Nation Enterprises*, 471 U.S. 539 (1985), the Supreme Court recognized that, although the unpublished status of a work was important, it was "not necessarily determinative" in considering a claim of fair use. *Id.* at 554. While a claim of fair use is not likely to prevail where a consumer widely distributes a full copy of a pre-release entertainment work, there may be other circumstances in which a claim of fair use could be appropriate. It is therefore be important to target illegal activity while maintaining the flexibility of the fair use doctrine.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.003

Questions from Senator Leahy

Q1. I have deep respect for privacy rights, and if there is an abuse of law, I believe that should be dealt with. Is there some use of the § 512(h) subpoena with which Verizon would be comfortable?

A1. Verizon has no objection to the use of the traditional Fed. R. Civ. P. 45 subpoena process in the context of a pending John Doe lawsuit, where a pre-service subpoena is subject to judicial supervision and subject to the Federal Rules of Civil Procedure. Further, Verizon does not believe that section 512(h) creates substantial privacy problems if the provision is limited to its original intended scope, where content is stored on a service provider's system or network. In that situation, the service provider has access to the content and may examine it, as contemplated by the take-down notice, which forms an essential part of the subpoena application.

Q2. Did Verizon raise any privacy concerns on behalf of its customers when it decided to support § 512(h) in 1998?

A2. Verizon was a leading participant in the 1998 negotiations, and specifically understood that section 512(h) was intended to apply solely as an adjunct to the take-down process available for material residing on the service provider's system or network in the context of subsection (c). That was the reason for the repeated cross references to subsection (c) and for the references in the required take-down notice to "material . . . to be removed or access to which is to be disabled." In that context, Verizon did not believe that section 512(h) raised substantial privacy concerns, because the material was publicly hosted on a provider's servers and it was expected that the service provider would have access to, and the ability to examine, the allegedly infringing material, and to judge the copyright owner's claim. The service provider would also have the ability to disable access to infringing material, providing more time for deliberative

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.004

judicial review. Further, Verizon understood that, in the subsection (c) take-down context, the sanctions for misrepresentation provided in subsection (f), and the counter-notification described in that subsection, would be available to further protect user interests.

Q3. To the extent that Verizon raised these concerns before, why did Verizon support the subpoena provision regardless of its concerns, and why do those privacy concerns now weigh more heavily?

A3. As discussed above, Verizon did not believe that, properly confined to the subsection (c) context, subsection (h) created substantial privacy concerns. Our concern with privacy arose out of the misconstruction of subsection (h) by the U.S. District Court for the District of Columbia, which enabled the sending of subpoenas in a context where the service provider often was unable to review the copyright owner's claim of infringement or remove specific material. Moreover, the District Court's construction could not logically be limited to peer-to-peer activity; it necessarily swept all conduit functions within the scope of subsection (h). Verizon believes that the conduit functions expressly considered by Congress in 1998 — anonymous web browsing and private email — were Internet functions where privacy and anonymity interests were at their zenith. The District Court decisions placed the privacy and anonymity of users of these Internet functions at risk. Fortunately, the D.C. Circuit corrected the District Court's error and the parties have been working amicably on enforcement activities ever since.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.005

Q4. Is there any way the parties can come together, as they did in 1998, to work out terms for the issuance and response to 512(h) subpoenas, which would satisfy everyone, and respect the privacy rights of individual customers? Could the parties agree to give notice to subscribers that their information is being requested, so that the subscriber could fight the subpoena if they wished?

A4. The parties did come together after the Court's unanimous decision and worked out a mutually agreeable process whereby RIAA could serve Verizon with judicially reviewed subpoenas and RIAA would take that information and contact the users directly. RIAA uses the information to send "pre-litigation" settlement notices to users and concludes that "[W]hat we've found is that more students tend to settle in the prelitigation stage, saving them from increasing costs that would otherwise occur if the legal process dragged on." RIAA Sees a 99.6% Capitulation Rate from Students at UT, http://arstechnica.com/news.ars/post/20080129-less-than-1-of-u-of-tennessee-students-hold-out-against-riaa.html, January 29, 2008. Those who do not settle are sued. RIAA has stated that its enforcement program continues to be a success, noting that the large number of lawsuits filed has "arrested the growth of a runaway solution that would have grown worse and worse." *See* RIAA's next moves in Washington, ZD Net, May 26, 2006, http://news.zdnet.co.uk/itmanagement/0,1000000308,39271312,00.htm.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.006

Questions from Senator Cornyn:

1. *The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would it even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), be amended, so that any reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. 506(a)(2)?*

Questions from Senator Leahy

1. *You stated in your written testimony that the peer-to-peer networks have made it difficult to track and investigate child pornography. Would you support requiring these networks to look for and report child pornography to your Center?*

ANSWER: Recent investigative breakthroughs within the Internet Crimes Against Children Task Forces (ICAC) have demonstrated that, if properly trained and equipped, law enforcement can identify the peer-to-peer distribution source of child pornography. Law enforcement ability to locate the machines distributing the images of child pornography can already outpace our national response capabilities to act on that information.

Therefore, I would propose a two-fold approach until our national response becomes more sophisticated in identifying the peer-to-peer distribution source. First, I would recommend that reports of the peer-to-peer distribution of child pornography be reported to the National Center for Missing and Exploited Children through the CyberTipline. Secondly, I would encourage the configuration of the software used in peer-to-peer systems to reject images of known child pornography from distribution. Some clients already contain filtering abilities.

Inevitably, there will be legal challenges to such configurations depending on how sophisticated the filtering technologies are regarding rejection of only known child pornographic images. However, the recent Supreme Court case involving the CIPA was resolved in favor of blocking and filtering strategies in publicly funded schools and libraries, even though some non-targeted material was also blocked.

2. *What other steps could be taken to respond to the problem of child pornography on Kazaa and other peer-to-peer networks?*

93014.007

ANSWER: From a legislative perspective, requiring Internet Service Providers to retain the Internet Protocol (IP) connection log information for a fixed period of 90 to 120 days would dramatically enhance law enforcements ability to track the origin of the images of child pornography. During the forensic examination of computers used to distribute child pornography over peer-to-peer networks it is common to locate IP information identifying the source of those images. Unfortunately, many providers do not retain the records long enough to be helpful in a criminal investigation. As an additional benefit, this requirement would also aid law enforcement in retrieving information during child abduction investigations where the victim had previous Internet contact with the abductor.

The analysis to this proposal may also require examining the financial costs to the ISP industry for maintaining such information for the required period of time.

3. *You mentioned in your written testimony that the peer-to-peer networks allow their users to remain anonymous while sharing child pornography. Have you found that the ability to exchange child pornography in a safe and anonymous atmosphere has an effect on the prevalence or severity of this pornography and on the exploitation of children?*

ANSWER: The very nature of the Internet allows many users to feel comfortable and anonymous while surfing online. For those engaging in online criminal activity, this anonymity may serve to lower their inhibitions and increase the likelihood of their offenses. Most users looking to exploit children online recognize that there is a law enforcement presence on the Internet. But, these offenders also recognize that there is a *very small* possibility of detection. Given the enormity of the Internet and the disparity between the number of offenders versus online police officers, child pornographers can trade their illegal images with little fear of detection.

The number of "new" child pornography images has dramatically increased in the last decade and the age of the victims is drastically dropping. There is an increasingly high volume of child pornography images featuring prepubescent children circulating online.

4. *Is there any other information of which the Committee should be aware concerning this problem?*

ANSWER: Additional funding for training, reporting, investigative and prosecutorial resources is critical. The speed that this technology allows child predators to exchange images of child pornography requires an equal and decisive response from law enforcement. Working to adapt to the present day challenges is not enough. We need to be able to obtain and retain the finest expertise in the field for law enforcement to anticipate and respond to this dynamic and ever-changing area of criminal enterprise. That means investing in systems upgrade, training and resources capable of identifying and archiving sufficient evidence to arrest and punish those who exploit our children through the devious use of technology.

93014.008

Answers to Written Questions from U.S. Senator John Cornyn
of the
United States Senate Committee on the Judiciary
Pornography, Technology, and Process: Problems and Solutions on Peer to Peer Networks

Tuesday, September 9, 2003, 2 p.m., Dirksen Senate Office Building Room 226

Question 1.

The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would it even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET Act, Pub.L. No. 105-147, 111 Stat. 2678 (1997), be amended, so that any reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. 506(a)(2)?

Answer to question 1:

I have some opinions but I'm not legally qualified to answer this question.

Question 2

I understand that, although important problems and concerns have indeed been raised, peer-to-peer (P2P) technology is nevertheless considered by many to be an integral component of the distributed architecture that is becoming increasingly important management in the 21st Century

> **a. Could you provide examples of data regarding positive uses of P2P technology?**

Answer to question 2a:

The Gartner Group says P2P will "radically change business models." Andy Grove, chairman of Intel, calls P2P "a revolution that will change computing as we know it." And vendors such as Lotus, IBM and Hewlett-Packard are rushing alongside Intel to build P2P applications. Yet this type of computing and its repercussions on the IT community are still not understood by many people.

P2P is a type of decentralized computing where computers communicate directly with each other, sharing resources, which don't necessarily connect with central servers or databases. P2P has actually been around for years in three areas, collaborative computing, instant messaging and affinity communities where direct file sharing occurs.

93014.009

Your question I'm sure refers to the last category. This will have great application for distributing research, teaching and other academic information.

Eric Garland of BigChampagne, a market research firm, predicts P2P will become the "go-to platform, a way to share proprietary information for banking, insurance, all industries. It's so efficient and robust, it will be applied to all types of online information."
Marty Lafferty, CEO of the newly formed Distributed Computing Industry Association, calls P2P "an incredible form of super distribution, not just for entertainment, but in ways to benefit humanity."

Hype or reality? Some examples:
BitTorrent. One of the best examples of P2P file sharing is BitTorrent which allows large, popular files to be downloaded quickly. BitTorrent has no network in the sense of KaZaA or Napster, it is a protocol. People or companies wanting to distribute a file essentially create their own private P2P network which only consists of whoever is down loading the file at the time. These miniature networks are formed around a "tracker", which is a server program operated by the entity who wants to share the file.

•**Data distribution.** Companies including Contiki and Akamai use P2P technology to help companies deliver sales presentations and multimedia content. Some banks already are using internal P2P to transfer data to branches. Television networks such as PBS are planning to use P2P to share programming between member stations.

•**Grid computing.** By linking a host of computers together to solve a problem, "You break the data into 1,000 pieces and solve the problem in a few days,"

•**Distributed file systems.** The files on a company network are broken into pieces and put into the P2P system, so if the server does go down, everyone's computers can work together to reassemble the files.

•**Collaboration software.** BadBlue allows home and business users to set up their own P2P networks. Groove Networks is similar, but more targeted to business. With a Web server, anyone who needs a piece of data has to contact one particular machine. With P2P, the media goes on multiple locations and can be accessed more quickly and efficiently.

You can see from these examples that P2P has great promise for quickly sharing important information and resources inexpensively and will provide back up on other peer machines when main servers fail.

b. To what extent are P2P software sellers able to track individual who use their software? Please describe how such tracking could work

Answer to question 2b:

93014.010

In the old days (2 years ago) the popular P2P protocols required that you register with the network and designate the content that you would be sharing, so the "owners" of the network would know who was sharing what content. Also when the P2P software was installed it would oftentimes install spy ware that could keep track of surfing habits, etc. of the user.

Many of the newer P2P programs (e.g. BitTorrent) are distributed and there is no real way to track who and how it is being used.

93014.011

QUESTIONS FOR WITNESSES FROM SENATOR LINDSEY GRAHAM "PORNOGRAPHY, TECHNOLOGY, AND PROCESS: Problems and Solutions on Peer-to-Peer Networks."

SEPTEMBER 9, 2003

Questions for Dr. Jacobson

1. You stated in your testimony that you "don't have to look for pornography on peer-to-peer networks; it will find you." When you log onto a P2P network and conduct a search, can you, in any way, get the information you want without accessing links to pornography files?

It depends on what files you run across during your search, since all you have to go by is the file name it is possible to download a file you think is a song and when you play it a web site pops up. It also depends on the peer-to-peer network you join. KaZaA does a better job of filtering out items that do not match their titles. Users rate the quality of the file and files that do not either match the title or are of low quality are given a low rating. Not all peer-to-peer networks even have logins, any one can join a gnutella network. The bottom line is that since you rely on the provider of the file for its content no file can really be trusted.

2. Do you think people are purposefully targeting children with pornography on these networks? If so, are peer-to-peer networks their method of choice and have they become the primary method by which pedophiles find their victims? If they are not presently the primary method, do you believe that they will become so in the future?

I think that pornography sites are targeting users on the peer-to-peer networks, and children. Peer-to-peer seems to be used to get pornography out in front of children (using key words like pokemon, Kate & Ashley, etc.) these files often contain not only pornographic pictures, but links to web sites. I do not think this is a method for pedophiles to find their victims since the goals of peer-to-peer are to help hide the users and to transfer files. There is not a good method (today) to use peer-to-peer for chat room types of activities. However, the peer-to-peer technology could support voice traffic and chat traffic. KaZaA does support instant messaging functions which would allow users to talk to each other. This could be used by pedophiles to talk to children that are using KaZaA, however they would have no way of knowing they were children unless they could guess by looking at the file names they downloaded. They could place files on their system with names that kids would like to download and then if someone downloads the files they could talk with them. This could also be a method for child pornography users to find out about each other. I see peer-to-peer becoming a secure and anonymous way to traffic in illegal materials like child pornography.

3. **You mentioned in your written testimony that the study Palisade Systems has been doing on peer-to-peer networks has shown pornography being downloaded at elementary schools. This makes one fearful of pedophiles using this to molest school children. What can law enforcement do?**

93014.012

Again, I'm not sure this a method for pedophiles to contact children, since it is used primarily file for sharing. Although if most schools block chat rooms then peer-to-peer could be used as another means of contacting children. There is the issue of exposing children to pornographic material. I think law enforcement can monitor peer-to-peer networks looking for child pornography and then deal with the individual(s) that are distributing it. I think there needs to be an awareness campaign to help schools understand the dangers of peer-to-peer. Most schools filter web sites, but do not filter peer-to-peer.

4. **In your written testimony you say that the newest steps in p2p networks is anonymous access, which is designed to hide the source of the information. Again, what tools does law enforcement need to actually go after the child predators hiding behind these p2p networks.**

This is the most difficult problem we face with peer-to-peer networks. Many of these anonymous sites are established in countries where U.S. law can not touch the people running the site. A possible answer would be to make it illegal to use an anonymous site that does not track the files (opened by court order). In addition we could look at methods to stop these "unauthorized anonymous" sites from sending files into the U.S.

5. **Finally you said that if a home user or parents allow these p2p systems to be installed that little can be done to prevent downloading of pornography. What there is your advice to parents. Should they not allow their children on p2p networks at all?**

My advise to parents is to not allow peer-to-peer traffic into their homes. There is no good use for peer-to-peer networks today. If they do allow peer-to-peer they need to carefully monitor what their children do on the network. I would also suggest a personal firewall which can provide some help with this problem. As I said the biggest thing is education.

6. **How can parents be empowered to go after the pornographers directly?**

Maybe some type of hot line. Again the problem is that not all of the pornographers are in the U.S.

7. **Do you think KaZaA and Sharman Networks' other businesses have duty to protect children using their service? If so, do you think they have done everything feasible to meet that obligation?**

Yes, they do have an duty to help protect children, I think that Sharman Networks has done several things to try and help solve this problem, like parent filters and user ratings. However, short of a central authority viewing of all files before they are posted (which is not the way peer-to-peer is setup to work) it is difficult for anyone to enforce content restrictions. The biggest problem is the peer-to-peer networks that do not have a company that produces the client software, but are produced by individuals that all follow the same protocol. When Palisade Systems did its first study we created a custom version of a gnutella client. Since it is up to the client software to enforce the filtering and not the actual peer-to-peer network all it takes is someone producing a client that will allow all data. You could write a KaZaA program that would not listen to the KaZaA filter rules and therefore allow all files to be transferred.

93014.013

Written Questions from Senator Leahy
Witnesses at the Hearing on Peer-to-Peer Networks
Senate Committee on the Judiciary
September 9, 2003

Questions for Douglas Jacobson

1. **From what you know of the Kazaa software, does it seem to you that the software is designed in such a way that helps users share child pornography anonymously and safely?**

   From what I can tell about KaZaA, it is not designed to provide anonymous access, which is why law enforcement has been able to track down child pornography distributors using KaZaA. I think the bigger problem is with other peer-to-peer networks like earthstation 5 which is designed to provide anonymous and encrypted access. The other complex issue is that we need to make a distinction between the client software and the protocol used. KaZaA is client software which speaks a certain protocol, just like there are over a dozen client applications that speak gnutella. Some protocols are designed to be anonymous while others are not. There are over 20 different peer-to-peer protocols used to transfer files between computers. Also many of the protocols that are designed not to be anonymous can be reworked to be anonymous, take the web for example, there are web sites that help hide who is making the web requests.

2. **Do any design components of Kazaa help law enforcement to track these child pornographers?**

   Nothing has been designed for that purpose, it is more of what they did not design into the protocol. Since they did not include anonymous access in their design the source of the files can be traced by law enforcement. However since it is a peer-to-peer protocol KaZaA has no control over the content being transfered.

3. **Is there some change the network could make that would make it easier to remove child pornography from the network?**

   They could look at tracking requests to see if people are requesting child pornography. I think they should set up a reporting system that would allow users to report child pornography they find on the network. That could be turned over to law enforcement. Again since the actual transfer is done between computers and does not involve Sharman Networks it is difficult for them to track the transfer.

4. **Is there any other information of which the Committee should be aware concerning this problem?**

   I think that the use of peer-to-peer networks for illegal activity will increase. I would be most worried about the peer-to-peer networks that we do not know about. Most peer-to-peer networks try to be inclusive and want as many users as possible. You could very easily set up a peer-to-peer network between a small number of computers and transfer material between them. The "private or hidden" peer-to-peer network would be a great way for people to communicate and if they used encryption their traffic could not be monitored. I also think that education is important, every user should know the potential dangers of peer-to-peer not only from a pornography standpoint but from a security standpoint. Companies should take steps to filter and closely watch for peer-to-peer traffic and other protocols that can cause security problems

93014.014

United States General Accounting Office
Washington, DC 20548

November 14, 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate

Subject: *Posthearing Questions from the September 9, 2003, Hearing on "Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks"*

Dear Mr. Chairman:

This letter responds to your September 17, 2003, request that we provide answers to questions relating to our September 9, 2003, testimony.[1] In that testimony, we discussed the availability of child pornography on peer-to-peer (P2P) networks. The questions posed by Senator John Cornyn and Senator Patrick Leahy to GAO, along with our responses, follow.

1. *Could you provide examples or data regarding potentially positive uses of P2P technology?*

Among the major uses of peer-to-peer technology are the following:

- *File sharing*, which includes applications such as Napster and KaZaA, along with commercial applications such as NextPage.[2] File-sharing applications work by making selected files on a user's computer available for upload by anyone else using similar software, which in turn gives the user access to selected files on the computers of other users on the peer-to-peer network.
- *Instant messaging (IM)*, which includes applications that enable online users to communicate immediately through text messages. IM

[1] U.S. General Accounting Office, *File-Sharing Programs: Users of Peer-to-Peer Networks Can Readily Access Child Pornography*, GAO-03-1115T (Washington, D.C.: Sept. 9, 2003).

[2] NextPage provides information-intensive corporations with customized peer-to-peer file-sharing networks. It enables users to manage, access, and exchange content across distributed servers on intranets and via the Internet.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.015

promotes a two-way conversational style of communication with minimal delay. Commercial vendors such as America Online (AOL), Microsoft, and Jabber offer free IM tools.

- *Distributed computing*, which includes applications that use the idle processing power of many computers. For example, the University of California–Berkeley's SETI@home project uses the idle time on volunteers' computers to analyze radio signal data. By taking advantage of the unused resources on volunteers' computers, the SETI@home project has been able to obtain more processing power than that available from the most powerful supercomputer for about 2 percent of the cost.

- *Collaboration applications*, which enable teams in different geographic areas to work together and increase productivity. Collaboration applications often combine single-function peer-to-peer applications, like IM and file sharing, into more complex applications. For example, the Groove application can access data on traditional corporate networks and on nontraditional devices such as personal digital assistants (PDAs) and handheld devices. This application offers IM, Web connectivity, and other add-on services.

2. *To what extent are P2P software sellers able to track individuals who use their software?*

The ability of peer-to-peer software vendors to track or regulate the use of their software depends on whether the peer-to-peer network is based on a centralized model, such as that used by Napster, or a decentralized model, such as the Gnutella[3] network used by KaZaA. In the centralized model, which is based on a central server or broker that directs traffic between individual registered users, it is possible for the administrators of the central server to track some of the individuals' activities by monitoring their interactions with the central server or database. In the decentralized model, in which individuals find and interact directly with each other, the ability of peer-to-peer software vendors to track individuals who use their software is greatly diminished. Any user of a decentralized peer-to-peer network,

[3]According to LimeWire LLC, the developer of a popular file-sharing program, Gnutella was originally designed by Nullsoft, a subsidiary of America Online (AOL). The development of the Gnutella protocol was halted by AOL management shortly after the protocol was made available to the public. Using downloads, programmers reverse-engineered the software and created their own Gnutella software packages.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.016

including the vendors of the software, can search the network to determine the files that are being shared on the network. However, according to one major software vendor, vendors of file-sharing software have no special ability to track or regulate the actions of the users of the software.[4]

3. *Are there any reasons why child pornography may be underreported on peer-to-peer networks?*

We do not know if the volume of child pornography on peer-to-peer networks is underreported. In our testimony, we cited the number of reports or tips received by the National Center for Missing and Exploited Children (NCMEC) as one indication of the volume of child pornography on peer-to-peer networks and on the Internet in general. NCMEC, a federally funded nonprofit organization that serves as a national resource center for information related to crimes against children, operates a CyberTipline that receives child pornography tips provided by the public; its CyberTipline II receives tips from Internet service providers. The Exploited Child Unit investigates and processes tips to determine if the images in question constitute a violation of child pornography laws and provides investigative leads to the Federal Bureau of Investigation (FBI), U.S. Customs, the Postal Inspection Service, and state and local law enforcement agencies.

As shown in table 1, in 2003 the NCMEC CyberTiplines received over 62,000 Internet-related reports of child pornography. Of these, 840, or about 1.4 percent, were related to peer-to-peer networks. However, we do not know if the number of reports received by NCMEC accurately reflects the volume of child pornography on peer-to-peer networks or on the Internet in general, since the reports are based on tips that the public or system users submit rather than a systematic analysis of network content.

[4] Statement of Mr. Alan Morris, Executive Vice President, Sharman Networks Limited, before the Senate Judiciary Committee regarding "Pornography, Technology and Process: Problems and Solutions on Peer-to-Peer Networks" (Washington, D.C.: Sept. 9, 2003).

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.017

Table 1: NCMEC CyberTipline (Internet-Related) Referrals to Law Enforcement Agencies, Fiscal Years 1998–2003

	Number of tips					
Technology	**1998**	**1999**	**2000**	**2001**	**2002**	**2003**
Web sites	1,393	3,830	10,629	18,052	26,759	45,035
E-mail	117	165	120	1,128	6,245	12,403
Peer-to-peer	—	—	—	156	757	840
Usenet newsgroups & bulletin boards	531	987	731	990	993	1,128
Unknown	90	258	260	430	612	1,692
Chat rooms	155	256	176	125	234	786
Instant Messaging	27	47	50	80	53	472
File transfer protocol	25	26	58	64	23	13
Total	**2,338**	**5,569**	**12,024**	**21,025**	**35,676**	**62,369**

Source: Exploited Child Unit, National Center for Missing and Exploited Children.

4. *Is there something particularly dangerous about the pornography on peer-to-peer networks, either in the user's ability to share it anonymously or in its accessibility to children?*

The pornography available on peer-to-peer networks is not necessarily more dangerous than the pornography available on Web sites or through other electronic means of dissemination. Although some users of peer-to-peer networks might believe that they are sharing files anonymously, it is possible for law enforcement officials to discover the identities of individuals sharing child pornography and other illegal material on peer-to-peer networks. With peer-to-peer networks, pornography is easily accessible to children and the risk of inadvertent exposure to pornography is significant. However, pornography is also easily accessible through other electronic means, such as Web sites, and the risk of children's inadvertent exposure to pornography exists on these other mediums as well.

5. *What steps does it take to keep child pornography off a peer-to-peer network?*

Preventing the introduction of child pornography on a peer-to-peer network would be very difficult, but legal means exist to investigate and prosecute those sharing this material on the network. Unlike traditional Web sites, which have centralized content management, users control the content that is available on peer-to-peer networks,

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.018

and the users of the network are constantly in flux. Nonetheless, law enforcement agencies can search peer-to-peer networks for child pornography and investigate reports of illegal material submitted to the NCMEC and other agencies. Once child pornography files are identified on a peer-to-peer network, legal mechanisms can be used to identify, investigate, and prosecute the individuals sharing the illegal files.

6. *The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would it even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), be amended, so that* any *reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. 506(a)(2)?*

The doctrine of fair use can apply to unreleased material. The fair use doctrine, which has been codified at 17 U.S.C. § 107, is available as an affirmative defense to those who infringe on copyrighted works that have yet to be released to the public. In order to respond to your question, we have interpreted your term "released," which is not defined under copyright law, to be equivalent to the term "published" under these laws. Although an infringing use of an unpublished work is less likely to be deemed fair by the courts, Congress amended the statutory codification of the fair use doctrine in 1992 to make explicit that the fact that a work is unpublished shall not itself bar a finding of fair use.

Under copyright law, it is not only possible but also plausible that a consumer could lawfully possess "pre-release" materials. For example, software developers frequently distribute "beta" versions of software programs for the purpose of "debugging" before the release of the program for retail sale. Any individual that the copyright holder intended to receive a work for a limited purpose would have a lawful right to its possession, notwithstanding that the material had not been released for sale to the general public. The subsequent distribution of such a work from an intended recipient might breach the terms the copyright holder set, if any, and could subject the recipient to civil and criminal penalties under copyright laws.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.019

Our work on peer-to-peer networks did not address issues concerning pre-release materials, and therefore we are unable to provide an opinion on the merits of amending the No Electronic Theft (NET) Act. We note, however, that the act's criminal penalties apply to all copyrighted works, regardless of whether they have been released to the public, and civil and statutory damages, up to $150,000 per infringement of a registered work, remain available to copyright holders regardless of whether the infringed work has been published or released (17 U.S.C. § 504). Further, in order to satisfy the threshold for a criminal infringement, the infringement must involve at least one copy, and the value of the total infringement must exceed $1,000 within a 180-day period (17 U.S.C. § 506). We understand that Senators Cornyn and Feinstein recently introduced legislation proposing to remove this threshold for criminal infringement.

In responding to these questions, we relied primarily on past work. We assessed the major uses of peer-to-peer technology, examined methods available to track the users of peer-to-peer applications, and reviewed the feasibility of controlling the content available on peer-to-peer networks. We also obtained updated information regarding the number of Internet-related Cybertipline referrals from the NCMEC. Finally, we reviewed and analyzed the applicability of the fair use doctrine of copyright law to pre-release copyrighted material.

Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-6240 or Mike Dolak, Assistant Director, at (202) 512-6362. We can also be reached by e-mail at koontzl@gao.gov and dolakm@gao.gov, respectively. Key contributors to this correspondence include Jason B. Bakelar and Lori D. Martinez.

Sincerely yours,

Linda D. Koontz

Linda D. Koontz
Director, Information Management Issues

(310392)

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.020

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 8, 2004

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

We have enclosed responses to questions posed by the Committee following the appearance of Assistant Attorney General John G. Malcolm before the Committee on September 9, 2003, regarding "Peer-to-Peer Networks and Child Pornography." We hope that you will find this information useful and that you will not hesitate to call upon us if we may be of additional assistance in connection with this or any other matter.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

**RESPONSES BY JOHN G. MALCOLM
TO QUESTIONS FROM THE
UNITED STATES SENATE JUDICIARY COMMITTEE
REGARDING "PORNOGRAPHY, TECHNOLOGY AND PROCESS:
PROBLEMS AND SOLUTIONS ON PEER-TO-PEER NETWORKS"
September 9, 2003**

QUESTIONS FROM SENATOR LINDSEY GRAHAM

1. You stated that the PROTECT Act law does not extend to file names that individuals create for files on their computers that they share on P2P networks. In your estimation, should the PROTECT Act be supplemented to address this issue?

Extending the Truth in Domain Names provision of the PROTECT Act, 18 U.S.C. § 2252B, to cover file names for shared files would likely prove ineffective for several reasons. Web site domain names exist by virtue of a paid registration with a domain name registrar, making the information about the individual who registered the domain name readily available (through legal process) at all times. By contrast, file names are selected by the individuals who share them, with no registration process, and the nature of P2P networks dictates that the identification of the IP address of the individual sharing the file must be identified in real time, *i.e.*, as the exchange is occurring. Thus, even if files were misleadingly named, it would be difficult to identify the culprit. In addition, names of shared files can be changed by anyone in the chain of distribution at any time, making it impossible to identify the person who misleadingly named the file. Moreover, an individual might unwittingly have a file in his or her shared folder (and therefore, available to others on the P2P network) that the individual has yet to view, yet has been misleadingly named by someone else.

Criminalizing the use of misleading file names would also fail to address those individuals who name their files accurately, yet alter the files' "metatag data," which are additional search matching criteria associated with the file. Thus, for example, a person can create a file containing pornography and name it as such, but alter the metatag data to include search criteria relating to a certain cartoon character, so that a child searching for that character will obtain the pornographic file. This metatag data can also be altered at any time by anyone sharing the file. For reasons similar to those described above, supplementing the Truth in Domain Names Act to include metatag data would likely prove ineffective in preventing this practice as well.

2. You mentioned that one of your biggest barriers to tracking and prosecuting distributors and viewers of child pornography is the fact that they do not use a central server when exchanging files. Are there currently any technological solutions to this problem? If not, what might we do to remove these obstacles for you?

The absence of a central server in P2P file sharing means that there is no central authority or presence on the Internet through which to track down illegal conduct retroactively. Rather, all investigations must be done as the exchange is occurring using online undercover techniques.

93014.022

This technological barrier would be difficult to remedy. Although P2P programs existed previously that did utilize a central server system (such as Napster), this type of P2P software is virtually non-existent now because of the potential liability attributable to the central server if individuals using the server are engaged in unlawful activity. There is also no incentive for those trading illegal files to return to the less anonymous central server system.

The secondary effect of the absence of a central server is that there appears to be no effective alternative mechanism for generating log records of file sharing transactions. The P2P software on each individual's computer does not generate log records, and if it did, no one would have access to that content except the individual computer owner, who would also have the ability to disable the record-keeping function or delete records altogether in order to secrete illegal activity. Thus, given the current state of technology, there appears to be no technological solution to the current P2P investigative barriers.

One way of overcoming the technological barriers inherent in P2P technology is to provide additional training for law enforcement officers. Not only is P2P technology relatively new and unfamiliar to many in law enforcement, but the method of investigating those who utilize P2P networks to disseminate child pornography and adult obscenity is different from the typical computer crime investigation. While some crimes involving computers are investigated reactively (by examining a suspect's computer hard drive to locate evidence of a past crime), P2P cases must be examined proactively (by using P2P software to obtain contraband files and then tracking down the user who distributed them). Additional law enforcement training on both P2P technology and the method of investigation, which the Department is endeavoring to undertake, would significantly enhance law enforcement efforts relating to P2P.

3. The Bureau has announced that it is currently considering a protocol for investigating child pornography cases on P2P networks. What is the current status of this project?

In conjunction with the Department of Justice's Child Exploitation and Obscenity Section, the FBI has developed a series of specific investigative techniques to be used in investigating child pornography transmissions through P2P networks. The FBI recently trained approximately 30 special agents from FBI field offices around the country on P2P technology and the FBI protocol for investigating P2P networks. This training will form the basis of the FBI's larger plan to decrease the proliferation of child pornography on P2P networks. In addition, several large-scale P2P investigations recently have been initiated as part of the FBI's Innocent Images National Initiative.

The Department of Homeland Security's Bureau of Immigration and Customs Enforcement (ICE) also reports that its Cyber-Crimes Center has initiated a pilot project that is part of Operation Predator and targets child pornography trading via P2P networks. The pilot project was initiated on September 8, 2003 and has already yielded at least sixty-two leads. Prior to this, several ICE offices were actively pursuing P2P investigations.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.023

4. Are so-called P2P "darknets" also becoming a problem in the distribution of pornography to children?

I understand the term "darknet" to be an informal term used to describe private file-sharing communities. The darknet is not a separate physical network but an application and protocol layer riding on existing networks. Examples of darknets are peer-to-peer file sharing, CD and DVD copying, Internet relay chat rooms, and key or password sharing on email and newsgroups. As I discussed in my testimony, the Internet is a target-rich environment, and criminal activity of all sorts, including the proliferation of child pornography, is occurring in all technological venues of the Internet. Certainly, as the Internet expands and technology develops, this problem will grow exponentially and will demand significant law enforcement attention.

5. What can be done to empower parents to deal with those specific individuals who share pornography files with their children?

A large part of empowerment for parents will be derived from their efforts to educate themselves about the Internet. Through no fault of their own, the current generation of parents was not exposed to computers in their youth, in sharp contrast to the children they are raising. As a result, parents tend to joke about their own relative computer illiteracy and assume that the Internet is safe or that their children understand enough about it to navigate it safely. Just as a responsible parent would not send off his or her young child alone on a city street peppered with adult book stores, hoping the child wouldn't enter, a responsible parent should not send his or her child alone onto the Internet, where children are even more capable of readily accessing pornography and even more vulnerable to the whims and advances of anonymous strangers.

In addition, there are technological tools and other materials that serve to protect children using the Internet. Many software companies sell blocking and filtering software that can be used to block access to, or filter out, unwanted materials. Indeed, some P2P software, including KaZaA, employs a "family filter" designed to avoid harmful files based on file names and/or metatag data. Though such filters are not perfect by any means, they do provide a first line of defense against pornographic materials. Many schools also have programs designed to educate children about the dangers of the Internet, and impose codes of conduct for Internet use by students. As well, the National Center for Missing and Exploited Children (NCMEC) provides educational materials on Internet safety, as do some, but certainly not all, ISPs.

6. Do you think KaZaA and Sharman Networks' other businesses have a duty to protect children using their service? If so, do you think they have done everything feasible to discharge that duty?

It is unclear whether this question speaks to a legal duty or a moral duty to protect children. Certainly, software manufacturers like KaZaA should strive to be good corporate citizens and do everything within their power to protect children who could otherwise be harmed through the use of their product. Unfortunately, however, good intentions on the part of the

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.024

software manufacturers are only part of the equation. A large part of the responsibility for protecting children on the Internet lies with parents, as discussed in response to the previous question. With respect to children who are given unfettered access to the Internet, there may be practical limitations on what software manufacturers like KaZaA can do. It is unclear whether the software manufacturing companies have any means to track what any particular user does with their software. It should be noted, however, that commercial products such as KaZaA are more likely to contain mechanisms intended to protect children than the many "clones" or functional equivalents of commercial P2P software that have been written by individuals and distributed over the Internet. In terms of whether P2P software manufacturers have done everything "feasible" to discharge their ethical and legal obligations, that is a question that I am not qualified to answer.

QUESTIONS FROM SENATOR JOHN CORNYN

For All Witnesses

1. The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would it even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET Act, Pub. L. No. 105-147, 111 Stat. 2678 (1977), be amended, so that any reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. § 506(a)(2)?

The fair use doctrine is designed to ensure that the protections afforded to authors and other creators by the copyright laws are properly balanced with the interest of the public in the free flow of information. The fair use doctrine allows people in certain circumstances to use copyrighted material in ways that the copyright owner has not authorized or approved, and even in ways that the copyright owner might forbid. Codified at 17 U.S.C. § 107, the fair use doctrine allows people to reproduce or otherwise use copyrighted works "for purposes such as criticism, comment, news reporting, teaching . . ., scholarship, or research" and other, unspecified, purposes and uses.

By design, the provision is fluid in nature and does not provide definite guidelines, but rather a multi-factor balancing test, to determine its applicability. In fact, it would be difficult to articulate a more determinate set of fair use rules, given the variety of copyrighted works, their varied uses, and the varied situations in which they can be used. Consequently, both through case law and statutory codification, fair use has historically been decided on a case-by-case basis looking at the totality of the facts at hand.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.025

It is clear, however, that the fair use doctrine can apply to copyrighted works that have not yet been released to the public. Congress made this point forcefully in 1992, when it passed the Act of Oct. 24, 1992, Pub. L. No. 102-492, 106 Stat. 3145. This act's sole provision and purpose was to amend 17 U.S.C. § 107 to say that "[t]he fact that a work is unpublished shall not bar a finding of fair use if such finding is made upon consideration of all the above [fair use] factors." The act's legislative history repeatedly underscores that Congress intends there to be no per se rule barring the fair use of unpublished works.

The legislative history illustrates that Congress took this step deliberately. It heard two days of testimony from the Register of Copyrights and those representing authors, publishers, computer companies, and the education community. According to the legislative history, biographers, historians, and publishers were concerned with court decisions that suggested that they could not use unpublished material of historical interest — such as the unpublished letters and diaries of major authors or public figures — in books or other serious treatments of historical figures and events. Congress heeded this testimony and thereafter amended the fair use statute to include the fair use of unpublished works.

The Department of Justice recognizes that there is a wide gulf between the serious historical scholarship that the act was intended to protect and the current practice by pirates of distributing music and movies before they are legitimately released to the public. However, it would be difficult to fashion a bright-line rule that criminalizes every use of unpublished, pre-release, copyrighted works in a way that is consistent with constitutional values, prior Congressional intent, and the policy of reserving Federal criminal prosecution for only the very worst offenders. A bright-line rule against use of unpublished works might, as Congress recognized earlier, punish any use of an unpublished work, even uses that are of significant social value (such as new reporting, criticism, scholarship, or research) and that adhere to traditional fair use limits on the manner and amount of copying. A bright-line rule could also punish speech that is arguably protected by the First Amendment.

That having been said, based upon current case-law, the Department believes that a claim of fair use is more difficult to sustain in the context of pre-release piracy than in regard to materials which are already published. The Department of Justice is unaware of any instance of criminal infringement that would have been prosecuted in the normal course of events but was not because the defendant raised a fair use defense in the context of piracy involving pre-release materials. In fact, on June 25, 2003, Kerry Gonzalez of New Jersey pleaded guilty to felony copyright infringement for uploading a pre-release version of the motion picture, "The Hulk," to the Internet in advance of the movie's release in theaters.

The Department of Justice recognizes, though, that the piracy of pre-release materials can pose significant adverse consequences and raise serious prosecutorial issues. Of particular concern is how to appropriately value pre-release products. The applicable laws, 17 U.S.C. § 506(a)(2) and 18 U.S.C. § 2319, measure the loss in copyright cases by using the legitimate retail value of the pirated products. It can be difficult to determine the retail value of pre-release

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.026

materials which, by definition, have yet to hit the retail market. Furthermore, copyright holders frequently claim that pre-release piracy damages them far more than the piracy of already-released materials. For example, the movie industry claims that pre-release piracy can destroy a film's opening box office take, which far exceeds the damage as measured by the retail price at which movie tickets or (looking even further down the line) DVDs will eventually be sold. This difficulty can be particularly problematic in the context of sentencing.

For John Malcolm

1. It is my understanding that, historically, the RIAA has expressed concerns that it would violate federal antitrust law for music labels to coordinate their efforts to combat Internet piracy and to promote online music solutions. In your view, are such antitrust concerns in fact valid? Would it be appropriate for Congress to craft an antitrust exemption to promote such coordinated efforts?

The Department's Antitrust Division advises that competitor collaborations and the market circumstances in which they operate can vary widely in their effects on competition. In enforcing the antitrust laws, the Antitrust Division seeks to give wide latitude to pro-competitive collaborations while challenging collaborations that would harm competition and consumers. Combating Internet piracy is a legitimate pro-competitive goal, and collaborative efforts in furtherance of that goal could be structured so as to keep any potential competitive harms – and potential antitrust exposure – to a minimum. Evaluating the legality under the antitrust laws of collaborative conduct among competitors requires a careful consideration of the exact nature of the conduct and its marketplace effects. The antitrust laws are a cornerstone of our free-market economy, and the Department has historically disfavored antitrust exemptions as harmful to competition and consumers.

QUESTIONS FROM SENATOR LEAHY

1. You described in your testimony some of the difficulties that law enforcement officers have in tracking and identifying the people sharing child pornography on peer-to-peer systems. Can you please describe the extent to which the design of these networks make it easier or more difficult for you to do your job?

P2P systems or "networks" are simply a group of individual computers sharing files with one another at any given point in time, which is facilitated by the use of P2P software. Because the computers generally communicate with one another directly rather than through a central server, there are often no log records of file transactions between P2P users. This likely absence of log records requires law enforcement to conduct investigations in real time by identifying the internet protocol (IP) addresses of persons sharing illicit files at the moment the files are being exchanged. Law enforcement authorities must then use legal process to obtain the identity of the individuals associated with those IP addresses. In addition, because an individual user's P2P

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.027

software installed on his computer generally does not keep log records of file transactions, if an individual's computer is seized and found to house file-sharing software and a shared file containing child pornography, it often will be difficult to determine through computer forensics whether the user ever accessed the files in the shared file after receiving them, which impacts the ability to prove knowing receipt, possession, or distribution of child pornography.

Moreover, P2P companies are promising that future generations of their software will provide users increased anonymity to shield users from detection and observation over the Internet by law enforcement and copyright holders. To make P2P users more anonymous, P2P software will use such techniques as encryption, port-hopping, proxy servers, and firewall-like features that screen out remote enquiries from watchdogs like law enforcement or copyright holders. While these tools may serve some legitimate purpose for those who use P2P networks responsibly, they will undoubtedly make those who abuse P2P networks harder to catch.

2. As you understand it, are those aspects of the network necessary to its functionality? Or are they something the networks could choose to remove?

The term "network" in the P2P context generally means a series of individual computers sharing files with one another at any given moment. Unlike the early versions of P2P (such as the now defunct Napster), current P2P systems generally have no central server. It is unclear whether the distributors of the software that allows individuals to share files on their computers (such as KaZaA) have any specific knowledge of, involvement in, or control over this activity. Thus, short of regressing to manufacturing software dependent upon a system with a central server (like Napster), it is possible that such companies are unable to remove or, so far as I am aware, create anything that would enable law enforcement to more easily investigate these cases, at least given the current state of technology. While Internet service providers, by contrast, could theoretically prevent files from being shared at the router level, this would undoubtedly impinge on the lawful trading of files.

That said, P2P software companies do have a choice as to whether they will offer their users anonymity. The techniques to achieve anonymity and thwart detection, which I have described in my answer to the previous question, are new additions to P2P software. They were not necessary for earlier generations of P2P software, and they are not necessary in the future. They are being added not to make the P2P networks work, but rather to make their work stealthier.

3. As you know, anyone "engaged in providing an electronic communication service or remote computing service to the public, through a facility or means of interstate or foreign commerce" is required by federal law to report all cases of child pornography on their networks to the National Center for Missing and Exploited Children. Under that definition, would peer-to-peer networks be covered by the statute, and if they would not, would you support amending the statute to cover them?

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.028

As discussed above, the term "network" in the P2P context generally does not connote a central authority with oversight over file sharing transactions, but rather, simply means a series of individual computers sharing files with one another at any given moment. As a result, it is unclear whether the distributors of the software that allows individuals to share files on their computers (such as KaZaA) have any specific knowledge of, involvement in, or control over this activity. So far as I am aware, they do not provide electronic communications services or remote computing services, and, therefore, do not fall within the mandate of 42 U.S.C. § 13032. Moreover, even if P2P software were technologically capable of allowing its manufacturers to monitor the activities of their users, and even if the manufacturers qualified as providers of electronic communications services or remote computing services, 42 U.S.C. § 13032(e) specifically states that providers have no duty to monitor the content of their users' communications.

In that the "networks" in the P2P context generally consist of ordinary citizens trading files, those individuals also do not fall within the mandatory reporting statute. Nevertheless, citizens do report the presence of child pornography on the Internet to the National Center for Missing and Exploited Children's Cyber Tipline, though this is purely voluntary.

4. The Department still has not issued procedural guidelines for Internet Service Providers to report cases of child pornography to the National Center. These guidelines will help reduce the amount of child pornography on the Internet, and will as a result make all children safer. I recently sent a letter to the Attorney General on this topic commending the National Center on its work and noting that these regulations are long overdue. When can we expect the Department to issue regulations concerning Internet Service Providers' responsibility to report this conduct?

The Attorney General is authorized to designate the law enforcement agencies to which reports may be forwarded by the National Center for Missing and Exploited Children (NCMEC), but the statute does not authorize implementing regulations to impose duties on Internet Service Providers (ISPs). *See* 42 U.S.C. § 13032(b)(2). Accordingly, the regulations can suggest, but not require, that ISPs report suspected violations in specific ways. The vast majority of large ISPs with whom the Department has consulted have indicated a desire to implement reporting in the manner most useful to NCMEC and the law enforcement community. The Department has been working with NCMEC, the FBI, the Department of Homeland Security's Bureau of Immigration and Customs Enforcement ICE), the United States Secret Service, the United States Postal Inspection Service, and the major ISPs to achieve consensus on the reporting protocols. This is a time-consuming process, particularly because of the technical constraints of both the individual ISPs and NCMEC that necessarily dictate the limits of any reporting protocol. On November 4, 2003, the Attorney General published the initial designation of four law enforcement agencies to which NCMEC should forward reports. *See* 28 C.F.R. 81.11 *et seq.* As the Department gathers a consensus on a more comprehensive set of guidelines both for ISPs reporting to NCMEC and for

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.029

NCMEC's reports to law enforcement, the Department will publish these operating guidelines. The Department appreciates the support of the ISPs in this endeavor and expects to be able to develop a consensus protocol.

5. Is there any other information of which the Committee should be aware concerning this problem?

I would like to raise two additional points. First, while it is true that P2P "networks" can be and are used to distribute child pornography, the problem spans many Internet venues. Indeed P2P may not be the most attractive Internet venue for this activity, because a person who makes files available for trade on P2P networks does not necessarily receive anything in return for the files he shares. From the user's perspective, more lucrative venues include commercial web sites, internet relay chats (IRCs), and newsgroups. Commercial web sites profit financially from providing access to child pornography to pedophiles. Likewise, IRCs allow users to profit in the form of mandatory file trading. Newsgroups facilitate similar file trading relationships between users. Thus, there are other means of communication on the Internet, in which child pornography proliferates, that arguably provide a stronger lure for offenders than do P2P "networks." While the instant inquiry into the use of P2P networks to distribute child pornography is an important one, the inquiry should not be limited to that venue alone, since child pornography is distributed, perhaps even more widely, through other Internet venues.

The second point I would like to raise is that it appears that a large number of ISPs are not fulfilling their mandatory reporting obligations under 42 U.S.C. § 13032. Of the approximately 7000 ISPs currently in existence, only a little over 100 of them are reporting the presence of child pornography on their servers to NCMEC. Most of these ISPs reporting are the larger, more prominent ISPs. It is highly unlikely that the roughly 6,900 ISPs are unaware of the existence of any child pornography on their networks. It is, in fact, likely that the non-reporting ISPs have a plethora of evidence that could aid law enforcement efforts to eradicate child pornography, were they to fulfill their mandatory reporting obligations.

QUESTIONS FROM CHAIRMAN ORRIN G. HATCH

1. Has any peer-to-peer network ever alerted you to the presence of child pornography on its network in order to aid you in enforcing the laws against child pornography?

The term "network" in the P2P context generally means a series of individual computers sharing files with one another at any given moment. Unlike the early versions of P2P (such as the now defunct Napster), current P2P systems generally have no central server. As a result, it is unclear whether the distributors of the software that allows individuals to share files on their computers (such as KaZaA) have any specific knowledge of, involvement in, or control over this activity. We are unaware of any P2P software companies reporting the presence of child pornography in files shared on the Internet. However, generally speaking, P2P software develop-

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.030

ers have been cooperative with agents investigating P2P "networks" and appear open to recommendations for software improvements. In addition, one P2P software manufacturer provided training on the use of P2P networks to ICE as well as software to assist in investigations.

Given that P2P networks consist of the individual users sharing files together, those individuals can report the availability of child pornography files to the Cyber Tipline at the National Center for Missing and Exploited Children (NCMEC). This reporting is purely voluntary. Although NCMEC does receive tips about the presence of child pornography on P2P networks, such tips are not useful to law enforcement unless the tipster provides the internet protocol (IP) address, obtained in real time, of the user from whom he downloaded child pornography.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.031

The Register of Copyrights
of the
United States of America

Library of Congress
Department 17
Washington, D.C. 20540

(202) 707-8350

September 30, 2003

Dear Senator Hatch:

Thank you for the opportunity to present the views of the Copyright Office at the United States Senate Judiciary Committee hearing regarding "Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks" on September 9, 2003.

Enclosed are my responses to the written questions from Committee members. If I can be of any further assistance in this, or any other matter, please do not hesitate to contact me.

Sincerely,

Marybeth Peters

Marybeth Peters
Register of Copyrights

Enclosure

The Honorable Orrin G. Hatch
Chairman
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, D.C. 20510

Response to the Written Question from Senator John Cornyn

1. The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), be amended, so that any reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. 506(a)(2)?

Response

Works which have not been released to the public will generally be considered unpublished works for purposes of copyright. Historically, Congress has respected an author's choice not to publish a work and afforded greater protection for such works. Indeed, prior to the enactment of the 1976 Copyright Act, unpublished works were protected by common law copyright so long as they remained unpublished, thus, potentially in perpetuity.

When Congress first codified the fair use doctrine into federal law, it was understood that:

> [t]he applicability of the fair use doctrine to unpublished works is narrowly limited since, although the work is unavailable, this is the result of a deliberate choice on the part of the copyright owner. Under ordinary circumstances the copyright owner's right of first publication would outweigh any needs of reproduction for classroom purposes.[1]

The Supreme Court addressed the application of the fair use defense to the use of unpublished works in 1985 and held that "[u]nder ordinary circumstances, the author's right to control the first public appearance of his undisseminated expression will outweigh a claim of fair use."[2] This language was strong enough that some believed it held that there is a "categorical presumption against prepublication fair use."[3]

In 1992, Congress acted to clarify the application of fair use to unpublished works, by amending section 107 to read, "The fact that a work is unpublished shall not itself bar a finding

---

[1] 4 Nimmer on Copyright §13.05[A][2][b]("Nimmer")(quoting S. Rept. No. 94-473, p.64 (1975).

[2] *Harper & Row, Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 555 (1985)("*Harper & Row*").

[3] Nimmer (quoting *Harper & Row* at 595 (Brennan, J., dissenting)).

93014.033

of fair use if such finding is made upon consideration of all the above factors."[4] The Report of this Committee in connection with that legislation provides an illuminating discussion of the events leading up to its enactment and I commend it to you.[5]

Thus, while the fair use defense clearly does apply to the use of unpublished works, a defendant will have a difficult case to make in order to overcome the second fair use factor,[6] which weighs against fair use in the case of unpublished works.[7]

With respect to your question regarding possession of pre-release materials by "ordinary consumers," some points must be kept in mind. First, where "ordinary consumers" possess copies of a work, it may suggest that the work has been published. For example, the distribution of promotional copies may satisfy the definition of "publication" in the Copyright Act.[8] Second, in general, the mere possession of copies does not violate any of the exclusive rights under copyright. Moreover, resale of *original, lawfully-made* promotional copies does not, in the absence of contractual terms to the contrary, infringe the distribution right.[9] However, in the case of promotional materials or pre-release copies, the Copyright Office is aware that there is a problem of unauthorized copying of such materials, followed by swift public distribution over peer-to-peer networks.[10] Such dissemination is likely infringing in several respects, because it involves the reproduction of copies without permission and public distribution of those unlawful copies.

I would add that it is difficult to conceive that the typical conduct of participants in peer-to-peer networks – downloading and make available for downloading the copyrighted works of others – would ever be considered fair use. While one might imagine some hypothetical situations in which the making available of a portion of another's copyrighted work (*e.g.*, in the context of a book review) on a peer-to-peer network could constitute fair use, I am not aware that such conduct often – or ever – occurs.

I would be inclined to support making the reproduction *and* distribution of "pre-release"

---

[4] Pub. L. No. 102-492.

[5] See S. Rept. No. 102-141 (1991).

[6] See 17 U.S.C. §107(2)("the nature of the copyrighted work").

[7] See Nimmer, n. 202.

[8] See 17 U.S.C. §101 ("Publication" is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending.")

[9] See 17 U.S.C. §109(a) (codifying the "first sale" doctrine).

[10] *See* Kenneth Terrell & Seth Rosen, *A Nation of Pirates*, U.S. News & World Report, July 14, 2003, at 40 (discussing the availability of the film Hulk before its theatrical release: "Two weeks before the film arrived in theaters, a version already was circulating online, available free to users of popular file-trading software").

93014.034

material acts that constitute criminal infringement, when the "pre-release" material is material such as a commercial sound recording or motion picture prior to its authorized distribution. I would be hesitant, however, to extend criminal liability to simply the reproduction of "pre-release" material unless it also involves dissemination of that material.

Response to the Written Questions from Senator Leahy

2. In your view, do Verizon's constitutional challenges to section 512(h) have any negative implications beyond the immediate context of the lawsuit?

Response

Verizon's constitutional allegations about the use of section 512(h) to identify infringers in the peer-to-peer context appear to be equally applicable in all the other contexts governed by section 512(h). For example, if there's no case or controversy where there is an allegation that someone on a peer-to-peer network is an infringer, I don't see how there could be a case or controversy where there is an allegation that someone whose website is hosted by a service provider is an infringer.

What this means is that Verizon and the others who are making these challenges to section 512(h) are, in effect, challenging it in all contexts. This appears to be a repudiation of the agreement made when section 512 was enacted.

When service providers came to Congress and asked for limitations on their liability, they asked that the burden of identifying infringing material be placed on copyright owners. The service providers argued that it was appropriate to do so because it would be a burden on them to monitor their own systems and, even if they could find possibly infringing materials on their system, they had no way to know what was protected by copyright or what was being used with permission. In contrast, copyright owners surely know what rights they own and what they have licensed and as such, it was argued, they were in a better position to identify infringing material. This is exactly what Congress did.

The logic is the same with regard to the subpoena process. Congress placed the responsibility to provide a limited amount of information to identify alleged infringers on service providers because it is information which they have and can provide, and which copyright owners otherwise would not be able to obtain.

Section 512 carefully balances rights and obligations. The subpoena is an integral piece of the effective and fair operation of that balance. As section 512 is written, the only relief copyright owners may obtain are injunctions against ISPs to prevent infringing material from being made available on that ISP's network. Without the subpoena process in section 512(h), there is nothing in section 512 that will help copyright owners to vindicate their rights against the direct infringers. I believe that Congress did not intend to create a system for dealing with online infringement that leaves such a gaping hole.

If section 512(h) is unconstitutional, all of section 512 should be declared unconstitutional, because section 512(h) cannot be severed without violating the intent of Congress and the expectations of the stakeholders who were involved in the discussions that led to 512. Service providers should not expect to enjoy the major benefits they obtained when section 512 was enacted if they are not willing to accept the few burdens that they agreed to.

93014.036

3. Verizon asserts that Title II of the Digital Millennium Copyright Act "was designed to protect Internet service providers from copyright liability in order to promote the growth of the Internet as a medium of political, social, and economic exchange." You were there when the Digital Millennium Act was being debated, negotiated, and enacted. Do you agree with Verizon's characterization?

Response

I agree that Title II of the DMCA was intended to promote the growth of the Internet, but not simply by "protect[ing] Internet service providers." That was only one mechanism through which Congress intended to promote the growth of digital networks. An equally important part of Title II was to encourage dissemination of high-quality copyrighted content, in part by fostering cooperation to eliminate infringing conduct on the Internet. Section 512 was designed to strike a balance that lets service providers run their businesses with certainty about how to handle copyright matters, respects the interests of those accused of infringement, and provides copyright owners with the ability to obtain redress for infringements of their rights. All of these interests were woven into section 512. As the House Commerce Committee wrote:

Title II [of the DMCA] preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.[11]

What concerns me is that the position Verizon is taking both before this Committee and in litigation seeks to undo an important part of that balance.

---

[11] H.R. Rep. 105-551, pt. 2, at 49-50 (1998).

93014.037

Response to Questions from Senator Lindsey Graham

How cooperative are ISP's in releasing identifying information to you for your investigative purposes? What are the challenges that you face dealing with ISP's?

We obtain subscriber and IP address information from ISP's by grand jury subpoena. We have developed good relationships with employees of the larger ISP's who are frequently very helpful in expediting responses to the subpoenas when necessary. We have not had an ISP move to quash any of our subpoenas to date.

The most significant problem we have with ISP's is the length of time it takes, absent exceptional circumstances, for them to respond to our subpoenas. I believe that this is really just a matter of volume. I do think that for the most part they make an effort to respond as expeditiously as possible.

Can you describe to me the typical profile of an on-line sexual predator and his usual methods of attracting unsuspecting children?

The typical profile of an on-line predator is a white male in his 30's. However, this profile did not fit the defendant's who were arrested in our recent investigation of the peer-to-peer file-sharing network KaZaA. These defendants were diverse in race, age and gender.

The usual method of attracting unsuspecting children is through chat rooms. After they text message in a chat room they go into "private" rooms and easily manipulate the conversation into one of a sexual nature.

Do you think KaZaA and Sharman Networks' other businesses have a duty to protect children using their service? If so, do you think they have done everything feasible to meet their obligations?

As I said in my statement at the hearing I believe they do have this obligation and clearly they have not done everything feasible to meet it. The quantity of child pornography on their networks is a testament to this fact.

93014.038

Response to Questions from Chairman Orrin G. Hatch

You testified that parents must be educated about the risks inherent in the use of peer-to-peer networks. As a law enforcement official, what methods or avenues of parental education do you think would be most wide reaching and effective?

I think a national campaign of clever, eye-catching public service announcements would be the answer. A campaign such as this could draw on the many talents of those in the music and film industries most affected by the peer-to-peer file sharing networks.

You also testified that file-trading networks should be held responsible for the illegal distribution of child pornography? Can you make any specific recommendations as to how to achieve that objective?

I believe that the only way this could be accomplished is by the passage of federal legislation. The passage of state laws, and the limits naturally imposed therein with respect to jurisdiction, service and the use of subpoenas and search warrants, would be ineffective.

Has any peer-to-peer network ever alerted you to the presence of child pornography on its network in order to aid you in enforcing the laws against child pornography?

No, not to my knowledge.

93014.039

Response to Questions from Senator Leahy

Your prosecution is breaking new ground, and I hope that it will serve as an example for law enforcement across the country. What types of problems have you faced in this investigation and prosecution?

As with any prosecution that breaks new ground there were challenges in developing the protocols for the investigation, drafting the search warrants and presenting the case to the grand jury. However, all of the problems, both legal and logistical, were able to be overcome because I was committed to and could dedicate the resources of my office to solving them. Many prosecutors do not have this luxury. Moreover, the Suffolk County Police Department has a dedicated computer crimes unit that was also fully committed to this investigation. Again, it would be almost impossible for many police departments to make this kind of commitment to an investigation of this nature.

In your view what can be done to make investigating and prosecuting child pornography easier?

Resources, resources, resources! Training, training, training!

You note in your testimony, correctly, that law enforcement can only do so much, and that steps must be taken to make it more difficult to share this type of material in the first place. In your view, what can be done to stem the tide of child pornography on peer-to-peer networks?

Somehow, the profit has to be taken out of it. I think that only after you make the owners of the networks both civilly and criminal responsible for what they carry will this happen.

Is there any other information of which the Committee should be aware concerning this problem?

I think the Committee has properly received information from the most knowledgeable sources available on this issue.

93014.040

QUESTIONS FOR WITNESSES FROM CHAIRMAN ORRIN G. HATCH

"PORNOGRAPHY, TECHNOLOGY, AND PROCESS:
Problems and Solutions on Peer-to-Peer Networks."

SEPTEMBER 9, 2003

Questions for Alan Morris:

1) Sharman's business partner, Altnet, requires a credit card to verify the age of anyone trying to access licensed pornographic materials distributed over the Kazaa network. Sharman is aware that much of the material on the Kazaa network is pornographic. Why has Sharman failed to configure its Family Filter so that it is activated until Sharman receives notice that an adult has authorized deactivation of the Family Filter?

2) Sharman's business partner, Altnet, requires a credit card to verify the age of anyone trying to access licensed pornographic materials distributed over the Kazaa network. Research indicates that from 20% to 35% of teenagers now have their own credit cards.

   a. Does Altnet verify whether a particular credit card holder is an adult or a minor, and if so, how?

   b. If a Kazaa user uses a credit-card to access Altnet-licensed adult or pornographic content, will the monthly statement for the card clearly indicate that the content purchased was pornographic? If the answer is "no," how can a parent determine whether a credit-card holding minor has purchased licensed pornography content from Altnet?

3) On September 12, 2003, searches of the Kazaa network using the terms "child porn" and "child rape" revealed numerous Altnet-licensed media files appearing at the top of the returned lists of responsive files.

   a. Has Sharman authorized Altnet to license the use of the Kazaa network to distribute media depicting child pornography or child rape?

   b. If Altnet-licensed media does not depict child pornography or child rape, (i.e., if the files contain misleading metadata), why does Sharman authorize Altnet to use Kazaa network to distribute pornography whose producers are trying to attract, and profit from, pedophiles?

   c. If Altnet-licensed media do not depict child pornography or child rape, (i.e., if the files contain misleading metadata), why does Sharman authorize Altnet to use Kazaa network to distribute files containing misleading metadata?

93014.041

4) Sharman maintains that it licenses networking technology that precludes Sharman from preventing Kazaa users from uploading pornography or child pornography disguised by misleading file names and/or metadata that enable those files to appear in response to even innocuous searches by users employing the Family Filter.

   a. What has Sharman done to warn Kazaa users and their parents that 1) the Family Filter cannot prevent exposure to misleadingly named and identified pornography or pornographic files, and 2) that Sharman has chosen not to prevent network users from placing misleadingly named pornographic files on its network?

   b. What has Sharman done to warn Kazaa users and their parents that even innocuous searches on the Kazaa network can retrieve child pornography that is illegal to view or possess?

5) Kazaa users have the option (enabled by default) to act as "Supernodes," in which case their computer may be selected to house part of a search index of files available for downloading over the Kazaa network. Peer-to-peer file-sharing services like Napster have been held liable for secondary copyright infringement, in part, because computers under their control maintained indices of infringing files available for trading over a peer-to-peer network. What has Sharman done to warn its users that persons allowing their computers to be used as Supernodes may expose themselves to risks of secondary infringement liability?

6) Please describe any future plans to add tools for additional user anonymity or additional encryption of communication, or other features which would make law enforcement's actions more difficult?

7) I understand that Kazaa uses hashes to uniquely identify content. If law enforcement provides the hash code of a file containing illegal child pornography, will Kazaa report all nodes offering that content, or provide a tool to law enforcement to identify all nodes? Will Kazaa modify the client software so super nodes can be instructed not to index the specified file? Is there a technological impediment to doing so?

8) A number of organizations, including the United States General Accounting Office, the U.S. Customs Cybersmuggling Center, and several private companies, have conducted studies of Kazaa and other peer-to-peer networks, during which they were able to locate illegal child pornography. What studies have you conducted of your network to locate illegal child pornography?

   a. If none, why haven't you conducted such studies in an effort to help law enforcement agencies enforce child pornography laws?

   b. If you have conducted such studies, how have you used the data?

9) What (other) proactive steps have you taken to rid your network of child pornography?

93014.042

Written Questions from Senator Leahy
to Witnesses at the Hearing on Peer-to-Peer Networks
Senate Committee on the Judiciary
September 9, 2003

Questions for Alan Morris

For answers that are different for Kazaa, KMD, Sharman Networks, or Altnet, please indicate what your answer is for each of these entities. Please do so even for questions that specifically name one of these entities. If you use any term of art, please define that term of art.

In addition to the questions concerning your testimony from the September 9 hearing, I am including and resubmitting to you the questions I asked after the June 17 hearing on the privacy and security risks posed by peer-to-peer networks. Each of these questions, from both hearings, asks for detailed information about specific aspects of Kazaa, and each is important to the ability of this Committee to do its work. Your responses, by contrast, lumped together all questions from a given topic and attempted to respond with generalities about that topic. Your responses, in short, were inadequate. Please answer each question asked of you, including the resubmitted questions, separately, fully and specifically.

1. What legal or other considerations led Kazaa to incorporate in Vanuatu?
2. Did you consider incorporating in the United States? Why did you not incorporate in the United States?
3. Did the desire to avoid legal liability of any type play any role in the decision to incorporate in Vanuatu?
4. How many people does Kazaa employ? Where are these employees located, and what functions do they serve?
5. What percentage of Kazaa employees work in Vanuatu?
6. Your product has serious and far-reaching consequences in the United States. Would you accede to the jurisdiction of the federal, state, and municipal courts of the United States for all purposes, including the attachment of property?
7. Would you agree to incorporate in the United States?

93014.043

8. As I mentioned to you at the September 9 hearing, 42 U.S.C. § 13032 states that entities "engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce" are required to report all cases of child pornography to the National Center for Missing and Exploited Children. You stated that you did not believe Kazaa was covered by this statute. Please explain why you believe that this language does not cover Kazaa.

9. Would you agree to abide by the reporting requirements of section 13032, regardless of the formal applicability of the statute?

10. I understand that you install on your users' computers software that tracks their activities online and puts advertisements on their hard drive, based on the information that this software collects about the individual user. If Kazaa does not do this now, has it ever done this? If there has been a change, why did the change occur?

11. How exactly does your company produce revenue? Please describe all sources of revenue and describe how any advertising works on Kazaa.

12. Does any advertising software on Kazaa collect any personal information about the user? If it does not do this now, has it ever done this? If there has been a change, why did the change occur?

13. If any advertising software did or does collect information about the user, does it collect information that would lead on to receive advertisements for pornography?

14. Does Kazaa sell any advertising space to pornography services?

15. Is there any way you can assure advertisers that their ads will not show up on the same screen as child pornography?

16. Do you make your advertisers aware of the fact that their ads very well may be running alongside pornography?

17. Is there any way you can assure your advertisers that their advertisements will not be interspersed with advertisements for pornography?

18. Is it technically feasible to give your users the ability to "tag" child pornography, so that law enforcement can find it easily and others can recognize it when they see it, and filter it out?

19. Will Kazaa add a one click function to allow users to report child pornography to the National Center for Missing and Exploited Children when they see it on your network?

20. Will Kazaa agree to give law enforcement authorities and the National Center for Missing and Exploited Children access to you network to monitor it for child pornography?

21. You contended at the September 9 hearing that the number of reported cases of child pornography on your network is small, but the recent Government Accounting Office report states that child pornography is prevalent on your network. Unlike other forms of distribution, your software makes it difficult for parents to monitor the content made available to their children, and difficult to get identifying information about the person offering it. Would you agree that these two factors explain the difference between the vast amount of pornography, child and otherwise, found by the GAO, and the low number of reports you cite? If you disagree, how would you explain the difference between your testimony and the findings of the GAO?

22. You make it more difficult for parents to keep their children off of your network, by designing your network to go around firewalls. This capability seems designed to thwart people's efforts to keep Kazaa out of their homes and off their networks. What legitimate purpose, if any, does this aspect of Kazaa's design have?

23. Is there any other information of which the Committee should be aware concerning this problem?

----------Page Break----------

Resubmitted Questions

For each of your answers, please indicate whether or not the answer will change in the new version (version 2.5) of Kazaa Media Desktop ("KMD"). For answers that will change, or that have changed, with the release of a new version of KMD, please indicate what your answer is for each of the versions. For answers that are different for Kazaa, KMD, Sharman Networks, or Altnet, please indicate what your answer is for each of these entities. Please do so even for questions that specifically name one of these entities. If you use any term of art, please define that term of art.

I. General

1. Do you agree that Kazaa, as the world's most popular peer-to-peer software, has an obligation to propagate a product that neither threatens a user's privacy, nor circumvents the various legitimate tools that people use to keep certain kinds of software and activities off of their systems?

II. Inadvertent File-sharing

The amount of inadvertent file-sharing that is occurring on Kazaa is disturbing. Your software apparently is leading many of its users to share materials that they almost surely would not knowingly share with the millions of other Kazaa users.

1. Does Kazaa in any way encourage users inadvertently to share personal information, and what steps is Kazaa taking to stop inadvertent file-sharing?

2. I understand that most people who have looked into this agree that this problem is created by misleading information in Kazaa's user interface. In fact it appears that your setup program is designed to encourage users to make the user's personal documents available to the public. Your setup window entitled "File Import," for example, is where the user decides which folders to share. Nowhere does this window tell the user that if a folder is selected, every file in that folder will be made available, whether it is an audio file, or a tax return. Also, in this window the "Search Wizard" option is highlighted, presumably to encourage the user to select it. This option automatically searches every drive available to a user's computer, and makes available any folder that has even one media or image file in it. This option is responsible for much of the inadvertent sharing of personal information on Kazaa. Why does Kazaa share every file in a folder with just one "qualifying" file in it?

3. Why does Kazaa not inform its users that, if a folder is selected for sharing, that in fact every file in that folder will be shared?

4. Why is the Search Wizard option highlighted, and by highlighting it, is Kazaa not encouraging users to give up their privacy, whether they know it or not?

5. One important aspect of the "Import File" window is not readily apparent to the user. Even though the Search Wizard is automatically highlighted, the default setting is actually not to use that option. Neither is the default the other option visible in this window. If the user simply clicks "OK," in this window he or she actually gets a third option. This is at best confusing, at worst deceptive. The standard practice in windows such as this is that the highlighted option is the one you would get if you click "OK." It is even more confusing if clicking on "OK" gives the user an option that is not even listed in that window. By deviating from the standard in this way, Kazaa is able to make many users think the Search Wizard is the default. It also allows you to claim that the "default" setting does not make personal files available, when in fact your software is geared to encourage users to do exactly that. Why does Kazaa deviate from the standard manner of informing the user what the default option will be in setting up file-sharing?

6. Why does Kazaa recursively search a user's drive for qualifying files, and make the entire contents of those folders available? Why does Kazaa not inform its users that it does this?

7. Why does Kazaa not allow its users to turn recursive searching off?

93014.046

8. In the "File Import" window of KMD's user interface, if the user chooses to take matters into their own hands and specify which folders will be shared, the user interface again is misleading. The window entitled "Browse for Folder" says that the user is choosing a "folder" for sharing, but does not inform the user that all of the folders selected and any sub-folders, plural, will also be shared. It also does not inform the user that by selecting a folder as the Download Folder, that folder also becomes the "upload folder," which is to say that every file in that folder will be available for sharing by everyone else on the network. Given the propensity for error in file-sharing, why does Kazaa use this misleading language?

9. When a user selects C:\ as the download directory, that will typically share the entire hard drive. If the C drive is chosen as the download directory on startup, Kazaa understandably warns the user about this, but if the download directory is *later changed* to the C drive, Kazaa does not warn the user, and in fact the sharing of the entire drive is not apparent in Kazaa's Folder Select window. Why does Kazaa not warn users when they change their download directory to share the entire hard drive, and why is the fact that a drive is being shared not apparentr in the Folder Select window?

10. In other ways Kazaa makes it difficult or burdensome to limit the sharing of files. For example, whereas an entire folder can be shared automatically if the Search Wizard finds just one qualifying file in that folder, to disable sharing the user must proceed file by file. Why does the My Media folder not allow users to stop sharing folders, but rather require that they disable sharing individually on a file-by-file basis?

11. One way users could be made aware of inadvertent file-sharing is if they could see that certain of their personal documents had been uploaded by others. KMD effectively prevents the user from discovering this, however, by "erasing" the transfer file interface each time the program is restarted. Given the fact that this is one of the few ways a user can tell what files have been uploaded from his or her computer, why does this not make it needlessly difficult for a user to keep track of his or her personal information?

12. At least one recent study has shown that the typical KMD user is in fact misled by Kazaa's user interface. Nathaniel Good and Aaron Krekelberg studied 12 individuals, 10 of whom had used file-sharing programs in the past, and all of whom spent considerable amounts of time on a computer. Those 12 went through Kazaa's entire interface. In the end only 2 of the 12 could tell which folders were being shared. The other 10 could not. Do you feel that 10 out of 12 users making an error that could seriously compromise their privacy is an acceptable number?

13. KMD's default settings seem to encourage the inadvertent sharing of files in other ways as well. For example, one default setting launches KMD when the computer starts. In fact, the default setting that achieves this seems purposefully worded so as to confuse the consumer. The option listed next to it is simply "family filter": in this option if the box is checked, the family filter is on. If it is unchecked, the family filter is off. The other option in the group is "Launch Kazaa Media Desktop after

93014.047

installation": if this is selected, KMD starts after installation. Both of these are very straightforward. The last option is different in syntax and logic. It reads, "Do not start Kazaa Media Desktop when the Computer starts." This asks the user to decipher two negatives, and figure out that to keep Kazaa from offering constant access to personal files the entire time the computer is on, the user must check this box. Moreover, the option appears right beneath an option that creates a quick launch button for KMD, further implying that some action is required on the user's part before KMD will launch. Why does the auto-launch option deviate from the straightforward wording of the other options, and why is the default setting that Kazaa will start when the computer does?

14. In the "My Kazaa" window, there is an option, already checked, called "Launch Kazaa Media Desktop automatically." Does this option mean that KMD will launch automatically the first time, after installation, or does it mean that KMD will start automatically every time the user's computer is turned on? If this option is effectively the same as the option described above (which launches KMD on computer startup), this could lead to confusion. In the case of a conflict between the user's responses to these two seemingly identical options, which option will take precedent?

15. Another KMD default is that sharing is enable on launch. Most KMD users presumably would like to control the amount of information they are sharing. Of course, they would also like to have access to as many different files as possible on the network. You have deliberately struck this balance strongly in favor of maximizing the amount of information available. You have done this in many of the ways listed here, but perhaps most strikingly by the simple fact that KMD's default setting is to share files, not protect them. What factors went into the decision to make sharing files the default setting?

16. Kazaa strongly encourages its users to make their computers and their bandwidth available for use by the Kazaa Network. In particular, KMD encourages users to serve as supernodes and to allow the maximum use of their bandwidth in the service of the network. The "advanced" tab of the KMD Options suite leaves the maximum bandwidth available for other users to download files from the user's computer, allows the user to function as a supernode, and selects "optimal" bandwidth when the computer is idle. Unlike all the other options, KMD tells the user only to change these default settings if the user "know[s] what they mean." If understanding these options is so important before changing any of them, does Kazaa explain these options to its user? Where does Kazaa offer an adequate explanation? Why does Kazaa specifically warn the user to retain these defaults, but not the others?

17. KMD users often find files by doing what is known as a keyword search, which will return any files that contain the word or words the user wants. However, once a file is found on a particular computer, an individual can do a search of everything on that computer, regardless of its subject. This makes Kazaa a powerful tool to discover a great deal of information about another user. At the same time, this function does not seem to greatly enhance an individual's ability to search for files related to a particular topic. For instance, if you type in the word "resume," and find someone's resume

93014.048

available, you can then select that person and get all of their files, including financial information like tax returns and medical documents. In light of the massive potential for misuse, why does Kazaa offer this function, and what is Kazaa doing to limit this type of data mining?

18. Why does Kazaa require its users to offer Kazaa for download, as opposed to uploading the program to those who would like to install it? Was any legal consideration taken into account in deciding to have current users offer the software for download?

----------Page Break----------

III. Firewalls and Security

Firewalls are important tools that allow parents to keep their children safe from online materials they have deemed harmful. They also allow network administrators to maintain some control over what activities take place on their network. Universities and government agencies use firewalls extensively to protect against unwanted sharing of sensitive information, and to keep programs that use a great deal of bandwidth from tying up their systems.

One common form of firewall controls access to a computer or network by limiting the ports that are available to the outside world. Port 21, for example, is a file transfer protocol port. Port 80 is the standard world wide web port, and so a firewall that intends to prevent file transfer protocol information from entering or leaving a system would block port 21, but would leave port 80 open. Because world wide web access is so important, even in the most restrictive firewalls it is almost always left open.

KMD uses the fact that port 80 is traditionally left open to get around this type of firewall. The window entitled "Kazaa Media Desktop Options" defines the ports that Kazaa will use to share information. Port number 1560 is the default port. But the default is that port 80 is the alternative port if port 1560 is blocked. This means that Kazaa is almost completely immune from port-blocking firewalls because so few will block port 80. In effect, if an administrator or a parent wants to stop Kazaa, he or she must block the Internet entirely or use a more complex and expensive form of firewall.

1. Why is port 80 chosen as the alternate port?

2. Did the fact that port 80 is left open by most firewalls play any role in Kazaa's decision to use that port as the alternate?

3. Does Kazaa have any other functions or attributes that allow it to circumvent any security measures?

93014.049

4. What steps is Kazaa taking to respect the rights of parents and network administrators to use firewalls effectively?

IV. KMD's End User Licensing Agreement

I have a number of questions about the manner in which KMD's End User Licensing Agreement ("EULA") informs KMD users of their rights and responsibilities, as well as the dangers of using KMD.

1. The EULA states that "if you are a minor you will become eligible to use Kazaa Media Desktop upon your parent or guardian reading and accepting the terms of this License." Why does Kazaa not state explicitly that minors *may not* accept the EULA, and why does Kazaa not confirm the age of the individual who agrees to the EULA, in light of the fact that there are relatively simple ways of doing so, such as requiring credit card information?

2. The EULA states that "your rights under this license will terminate immediately and without prior notice if: you violate any term of this license, including violating any applicable laws or rights of any third party including the intellectual property rights of any such third party. You may be subject to legal action if you continue to use the Kazaa Media Desktop in violation of this License." Why does the EULA terminate under these circumstances? Has Kazaa ever taken any action under this provision of the EULA?

3. Why does Kazaa place four different sets of important terms, including the EULA, the privacy statement, adware and spyware, and usage of resources information , in one window, as opposed to encouraging the user to consider each of these important documents separately?

V. KMD's Privacy Statement

1. KMD's Privacy Statement states that, although KMD will occasionally request personal information about its users in furtherance of surveys or contests. It states that "[c]ontact information will be shared with the contest or survey sponsors to notify the winners and award prizes or otherwise in accordance with the Terms and Conditions of each competition or survey." This implies that the primary use of the information collected will be to notify winners. Is it typical that the information is used only to notify winners, or are other uses common?

2. You state that "Usage of a cookie is in no way linked to any personally identifiable information while on our site or using KMD." Are the cookies you install ever linked with personally identifying information?

93014.050

3. You state that "Sharman Networks has no ability to supervise, control or know your activity." Does this statement include information collected by the adware/spyware that Kazaa installs? Does it include such content restrictions as the family filter? When Gnutella left the Sharman Networks, you forced Gnutella users off of your network by pushing an update to the other Sharman users, but not Gnutella users. Would the ability to remove a user from the network be included in "supervision or control" of usage?

4. KMD states that "[u]sers are given the opportunity to 'opt-out' of having their information used for purposes not directly related to our site at the point where we ask for information. For example, the KMD options screen has an 'opt-out' mechanism so users who don't want any marketing material, can keep their email address off our lists." In fact, may a user opt out of the installation of the adware/spyare that collects user information? Does choosing not to give one's email address actually prevent the receipt of "marketing material"?

5. KMD states that "Other users may download files that you have stored in the My Shared Folder and other folders you have specifically selected to be shared." Does this adequately describe the availability of folders that have been found by the search wizard? Does it adequately describe the effect of recursive searching?

6. KMD states that "the Cydoor component uses your Internet connection, which was designed to take up the minimum amount of bandwidth on your line." Does this mean that Cydoor was designed to use minimal bandwidth, or that the Internet connection was designed to use minimal bandwidth?

7. In describing the effect of Cydoor's storage of banner ads on a user's hard drive, KMD states that "[e]ach ad banner on your hard disc is about 10Kbytes." Why does KMD not tell the user how many ad banners are stored on a user's drive at any given time?

VI. Virus Protection

1. You have stated in the recent Senate Judiciary Committee hearing and in other testimony that Kazaa offers powerful virus protection and in fact you state that Kazaa takes "every opportunity to encourage responsible and safe peer-to-peer usage through user education as well as via the default configuration of the software." Indeed, the front page of the KMD website attempts to alleviate a potential users' security fears. It states with respect to KMD's anti-virus software, "once enabled, Bullguard Lite provides virus protection when using KMD." However, KMD's default is for Bullguard to be turned off. In addition, elsewhere you warn the user not to change the security settings. Thus, Kazaa actually discourages the user from turning on the virus protection you have described and on which your users rely. In light of this default setting, KMD's

93014.051

warning not to change it, and the fact that there have been at least eight major virus outbreaks on Kazaa, does Kazaa adequately protect its users from viruses?

2. Has Kazaa performed any analyses of the propgagtion of viruses over the network?

3. Does Kazaa take any steps to control or monitor viruses on the network? Please describe any such steps.

VII. Spyware and Adware

Spyware and adware are data collection software that collect all sorts of information about the user, like where he or she is going on the Internet, what search terms they enter, and html content. Spyware is typically defined as software that is installed on a user's computer with no notice to the user. Adware is installed with some notice. I understand that your position is that Kazaa does not install "spyware," because there is a reference to this software buried deep within your license agreement. However, it seems from the license agreement that the user must actually seek out the relevant information about the programs that Kazaa installs on its users' computers. In addition, the software you install is set to run the entire time a user is on his or her computer, not just when they are using Kazaa.

1. Why does KMD not explain in clear terms what the user is agreeing to, and what this software will do?

2. Why does KMD not explain how difficult it will be to remove the spyware/adware?

3. What steps is Kazaa taking to ensure that users can quickly and easily uninstall this software?

4. Why does KMD not explain that the spyware/adware continues to run even when Kazaa is not running?

5. WhenU.com, the distributor of SaveNow, one of the spyware/adware programs that are automatically installed with Kazaa, is explicitly not available to those under 13 years of age. Since Kazaa requires the installation of a WhenU product in order for it to be launched, Kazaa in effect requires that its users be at least 13 years of age. Nonetheless, Kazaa does not require proof of age. Do other applications that bundle SaveNow require a proof of age?

6. What methods of proof of age are feasible?

93014.052

7. The End User License Agreement requires the user to agree to accept any future updates or upgrades to the software. How does Kazaa and/or WhenU update or upgrade the software once it is installed on a user's computer?

8. Is this method of updating or upgrading feasible for updating or upgrading the software the KMD software? Are update or upgrades performed in the same manner for KMD and the adware/spyware that comes bundled with KMD?

93014.053

QUESTIONS FOR WITNESSES FROM SENATOR LINDSEY GRAHAM

"PORNOGRAPHY, TECHNOLOGY, AND PROCESS:
Problems and Solutions on Peer-to-Peer Networks."

SEPTEMBER 9, 2003

Questions for Mr. Morris.

1. Sharman Networks, through Altnet, is a commercial distributor of pornography. What warnings or procedures have you installed that ensure that pornography is only available to adults? Do you consider these measures adequate?

2. What responsibility is KaZaA willing to take, above and beyond what they are already doing at this time, to protect children, their primary users, from harmful adult pornography and illegal child pornography?

3. What is your opinion on the following proposals to limit P2P pornography distribution to minors?
- Requiring off-network notice to parents of the pornography threat to their children.
- Simplified "uninstall" procedures.
- Allowing users to decline "supernode" status for their computers.
- Requiring P2P services to maintain an agent for service of process in the US.
- Network recognition of "do not install" beacons.

4. Do you think KaZaA and Sharman Networks' other businesses have duty to protect children using their service? Do you think you have done everything feasible to meet that duty?

93014.054

United States Senate
Committee on the Judiciary

U.S. Senator John Cornyn

Pornography, Technology, and Process:
Problems and Solutions on Peer-to-Peer Networks

Tuesday, September 9, 2003, 2 p.m., Dirksen Senate Office Building Room 226

WRITTEN QUESTIONS FROM SENATOR JOHN CORNYN

For Alan Morris

1. I understand that, although important problems and concerns have indeed been raised, peer-to-peer (P2P) technology is nevertheless considered by many to be an integral component of the distributed architecture that is becoming increasingly important for information management in the 21st Century.

(a) Could you provide examples or data regarding potentially positive uses of P2P technology?

(b) To what extent are P2P software sellers able to track individuals who use their software? Please describe how such tracking could work.

1. Can you tell me what specific actions your company can take in the future to prevent children from sharing illegal files, whether they are pornographic or copyright protected material? Please provide specific, concrete proposals.

1. The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would it even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), be amended, so that any reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. § 506(a)(2)?

93014.055

Written Questions from Senator Leahy
to Witnesses at the Hearing on Peer-to-Peer Networks
Senate Committee on the Judiciary
September 9, 2003

Questions for Cary Sherman

1. What considerations did you take into account when you supported the subpoena provisions that were eventually embodied in section 512(h)?

2. What steps do you take before issuing an information subpoena pursuant to 512(h)? How can we know that your clients request this information only when they reasonably need to do so?

3. Is there any way the parties can come together, as they did in 1998, to work out terms for the issuance and response to 512(h) subpoenas, that would satisfy everyone, and respect the privacy rights of individual customers? Could the parties agree to give notice to the subscribers that their information is being requested, so that the subscribers could fight the subpoena if they wished?

93014.056

Senator Saxby Chambliss
Written Questions for Witnesses at September 9, 2003 Hearing
Senate Judiciary Committee
"Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks."

Questions for Cary Sherman
President, Recording Industry Association of America (RIAA)

Q. How is RIAA deciding whom to sue? What suits have been brought to date? How many suits are you planning to file?

Q. Have you contacted the people who were subpoena targets? How many of them? What means of communication have you used? Can you share whether anyone responded in a manner such that RIAA felt they did not need to sue?

93014.057

United States Senate
Committee on the Judiciary

U.S. Senator John Cornyn

Pornography, Technology, and Process:
Problems and Solutions on Peer-to-Peer Networks

Tuesday, September 9, 2003, 2 p.m., Dirksen Senate Office Building Room 226

WRITTEN QUESTIONS FROM SENATOR JOHN CORNYN

For Cary Sherman

1. It is my understanding that, historically, the RIAA has expressed concerns that it would violate federal antitrust law for music labels to coordinate their efforts to combat Internet piracy and to promote online music solutions. In your view, are such antitrust concerns in fact valid? Would it be appropriate for Congress to craft an antitrust exemption to promote such coordinated efforts?

1. The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would it even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), be amended, so that any reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. § 506(a)(2)?

93014.058

SUBMISSIONS FOR THE RECORD

Statement of William Barr
Executive Vice President and General Counsel
Verizon Communications

Before the United States Senate
Committee on The Judiciary

Pornography, Technology and Process: Problems and Solutions on Peer-to-Peer Networks
September 9, 2003

Mr. Chairman and members of the Committee, thank you for inviting me here today to discuss this important issue.

We at Verizon recognize the legitimate interests of copyright owners and the threats to those interests that are posed by the misuse of new technologies, including peer-to-peer software. Verizon remains committed to working with the copyright community to find solutions to these issues that result in effective protection for intellectual property, without placing substantial burdens on Internet service providers or violating the privacy and First Amendment interests of their subscribers. Back in 1998, Verizon and other service providers agreed in the Digital Millennium Copyright Act ("DMCA") to conduct voluntary industry negotiations aimed at developing "standard technical measures" (also known as digital rights management tools), to protect copyright works from online infringement.[1] The copyright community has never accepted our offer to begin those negotiations and to work cooperatively toward a technical solution to this problem. In the end, as in the area of VHS recordings and cable television access to broadcast programming, Verizon believes that appropriate technical and legal solutions will be

[1] 17 U.S.C. 512(i)(1) & (2).

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.059

found. As discussed in detail below, the district court's misreading and misapplication of the Section 512(h) subpoena power is not that solution.

As an Internet service provider, Verizon promptly takes down infringing material that resides on our system or network in response to requests from copyright owners and we have strict policies against infringement of copyrights. Verizon also promotes legitimate pay music sites such as MP3.com and Rhapsody as part of its ISP service. We will continue to work with copyright owners to marry the power of the Internet with the creative genius of content providers through new business relationships and licensed websites that offer music, video, and other proprietary content to the over 100 million Internet users in this country. Verizon believes that lawful and licensed access to quality content is essential to the continuing development of the Internet in general and broadband in particular, and we are committed to exploring technological and other solutions so that copyright owners may enjoy the fruits of their labors and Internet users will have access to a rich array of digital content.

However, the answer to the copyright community's present business problems is not a radical new subpoena process, previously unknown in law, that un-tethers binding judicial process from constitutional and statutory protections that normally apply to the discovery of private data regarding electronic communications. Verizon believes that the district court was wrong in concluding that Congress authorized such a broad and promiscuous subpoena procedure in the DMCA—but whatever the courts ultimately conclude on this issue—the subpoena power endorsed by the district court is not an effective remedy for copyright holders and has great costs in terms of personal privacy, constitutional rights of free expression and association, and the continued growth of the Internet.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00110 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.060

As interpreted by the district court, this subpoena provision grants copyright holders or their agents the right to discover the name, address, and telephone number of any Internet user in this country without filing a lawsuit or making any substantive showing at all to a federal judge. This reading of the DMCA accords truly breathtaking powers to anyone who can claim to be or represent a copyright owner; powers that Congress has not even bestowed on law enforcement and national security personnel. It stands in marked contrast to the statutory protections that Congress has enacted in the context of video rentals, cable television viewing habits, and even the requirements for law enforcement officers to gain access confidential data associated with electronic communications.

All one need do is fill out a one-page form asserting a "good faith" belief that a copyright has been infringed and one can obtain identifying information about anyone using the Internet. There is no review by a judge or a magistrate; the clerk's office simply issues the subpoena in ministerial fashion. This identifying information can then be linked to particular material sent or received over the Internet, including e-mails, web browsing activity, chat room postings, and file-sharing activity. It is also important to remember that the threshold for a claim of copyright in any form of expression is extremely low. This subpoena power applies not just to sound recordings, it applies to the expression contained in an e-mail or posting in a newsgroup, digital photographs, and even pornographic materials. It has and will be used and abused by parties far less responsible than the recording or movie industries. In essence, any private party willing to assert a property right in any form of expression is constituted as their own roving grand jury, without any of the normal checks and protections that apply to governmental investigations.

Under our constitutional scheme, the issuance and enforcement of judicial process in civil cases is generally confined to an actual case or controversy and is undertaken under judicial

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00111 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.061

supervision. The district court's reading of Section 512(h) departs from this constitutional tradition and thus eliminates many of the normal constraints on discovery by civil litigants. The statute lacks the most basic protections that are applied to the discovery of confidential and personal data connected with expressive activity. As noted above, the filing that need be made is truly minimal, and is below the notice pleading standard for the filing of a civil complaint in federal court. The normal duties to investigate and substantiate a civil claim that apply to the filing of a lawsuit under the Federal Rules of Civil Procedure do not apply. The clerk's office simply rubberstamps these subpoenas in ministerial fashion—with no inquiry into the bona fides of the party filing the request or the self-interested "belief" that a copyright has been violated.

The individual subscriber, whose identity is at issue, is not even entitled to receive notice of the subpoena before his or her personal information is turned over to a third party. Thus, the subscriber, who may in fact be engaged in fully protected speech or association, will have his or her identity revealed without ever having an opportunity to be heard in court. There is no opportunity to assert the normal defenses to a claim of copyright infringement—fair use, the non-protection of ideas, or the fact that material resides in the public domain. Nor is there any provision for damages or other punishment for wrongfully obtaining or misusing the identity of a subscriber subject to such a subpoena. It is truly ironic that Congress has placed more substantial requirements and protections on law enforcement access to confidential information regarding electronic communications than apply to a private party under this statute.[2] Given the substantial privacy protections that Congress built into the DMCA itself, *see* 17 U.S.C. § 1205 (savings clause for state and federal privacy laws); *id.* § 512(m) (protection of subscriber privacy

[2] *See, e.g.*, 18 U.S.C. § 3121, *et seq.* (pen registers and trap and trace devices limited to governmental personnel upon court order for valid criminal investigation); 18 U.S.C. § 2703 (limits on disclosure of records pertaining to electronic communications services).

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00112 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.062

from monitoring of Internet communications) it is utterly implausible that Congress wished to create this substantial threat to personal privacy in the subpoena provision contained in the same statutory scheme.

This combination of unlimited scope, minimal substantive requirements, and lack of judicial supervision makes both mistakes and intentional abuses of this new power inevitable. Every time you send an e-mail, browse a website, or join a discussion in a chatroom or newsgroup, others gain access the numerical IP address that you are using. Armed with this IP address, anyone to whom you have sent an e-mail, from whom you have received an e-mail, with whom you or your children have spoken in a chat room, or who operates a web site you have visited, no matter how sensitive the subject matter, can unlock the door to your identity.

This list is not limited to those with legitimate interests in enforcing copyrights. As safety and privacy groups like the National Coalition Against Domestic Violence and WiredSafety stated in our litigation, it opens the door to your identity to people with inappropriate or even dangerous motives, such as spammers, blackmailers, pornographers, pedophiles, stalkers, harassers, and identity thieves. In fact, over 92 diverse organizations, representing consumer and Internet interests, submitted letters to this Committee last week expressing serious concerns about the privacy, safety, and security of Internet users arising from the potential misuse of this subpoena process. These include the ACLU, the American Library Association, the Consumer Federation of America, and the National Coalition Against Domestic Violence. These groups do not condone copyright infringement rather, like Verizon, they are concerned that this subpoena provision will cause great harm to privacy, free expression, and even personal security of Internet users with little gain in copyright enforcement.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00113 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.063

As Ms. Aftab, from WiredSafety states, "With one broad sweep, the DMCA subpoena power will frustrate the work of the entire online safety community to arm our children and their parents with cyber-street-smarts. It won't matter what they voluntarily or mistakenly give away. All the information predators need can be obtained far more easily with the assistance of the local Federal District Court Clerk." The potential for abuse of this new subpoena power is limited only by the deviousness of the criminal mind.

Indeed, just since the district court's ruling went into effect in June, the evidence of mistakes, potential abuses, and troubling uses of this subpoena power has continued to mount. SBC recently filed a suit in California against the Recording Industry, a copyright bounty hunter called "MediaForce" and an entity called Titan Media Group. Titan Media, a purveyor of pornographic videos over the Internet, sent one subpoena to SBC seeking the names, addresses and phone numbers of 59 individual subscribers who Titan asserted were infringing its copyrights in gay pornographic videos by exchanging them over the Internet. Titan eventually withdrew the subpoena when SBC threatened a court challenge, but the episode highlights the fact that this new subpoena power applies to *anyone* who can claim an interest in *any* form of expression. In a similar vein, ALS Scan, a purveyor of graphic Internet pornography, has also used the DMCA notice and takedown process and in fact submitted a declaration in favor of RIAA's broad interpretation of the subpoena power in the litigation with Verizon. The potential for abuse, for invasion of personal privacy, for reputational harm, and even for blackmail is highlighted by these examples.

The statute does not even require the copyright owner itself to obtain the subpoena, it may be obtained by an agent of the copyright holder. A whole industry of copyright "bounty hunters" has sprung up, enterprises that search the Internet for possible instances of copyright

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00114 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.064

infringement spurred on by economic incentives. The use of automated robots, known as "bots" or "spiders" has also led to a significant number of mistaken claims of copyright infringement. These bots operate much like the spiders that crawled through buildings in the movie Minority Report, scouring the Internet in search of file names that look like they match the names of copyrighted works or artists. Bots are far from perfect. Typing words such as "Madonna" or "the police" in an e-mail may earn you a DMCA subpoena, because the "bots" cannot distinguish the legitimate comment or discourse from copyright infringement. In 2001,Warner Bros. sent a letter to UUNet demanding that they terminate the Internet account of someone allegedly sharing a Harry Potter movie online. The small text file was entitled "Harry Potter Book Report.rtf., with a file size of 1k. The file was not an unauthorized copy of the movie, it was a child's book report, but the bot could not tell the difference and such an "investigation" can quickly form the basis for a DMCA subpoena.

In the past few months, RIAA has already admitted numerous cases of "mistaken identity." In one case, RIAA demanded the take down of Penn State University's astronomy department's servers during finals week, based on a claim that it contained infringing songs by the artist Usher. In fact, "Usher" is a professor's last name and the file at issue was his own creation. RIAA later admitted sending at least two dozen other mistaken notices to Internet users as part of its campaign to warn peer-to-peer file-sharers. And this was before RIAA began its new campaign sending hundreds of subpoenas for subscriber identity to ISPs across the country. These chilling examples all sound like excerpts from the book "1984," except in this case, "Big Brother" isn't the Government, it is interested parties armed with their own private search warrants.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00115 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.065

RIAA's most recent campaign began in July of this year after the district court's ruling went into effect. Despite the pending appeal on this issue, the Recording Industry has chosen to unleash numerous subpoenas on Internet service providers. Verizon has already received nearly 200 subpoenas, with which we have been required to comply. The Recording Industry alone has sent well over 1000 subpoenas to service providers across the country, placing a significant strain on the resources of the clerk's office of the district court in D.C. and on the subpoena compliance units at many Internet service providers, including Verizon.[3]

RIAA now claims that it is entitled to discover subscriber's e-mail addresses through these subpoenas and further claims that it may issue these subpoenas from the district court in Washington D.C., regardless of the location of the service provider or the customer. Obviously, obtaining the subpoena in a distant forum makes it a practical impossibility for many service providers and most customers to ever raise any objection to the subpoena. Indeed, Boston College and MIT successfully fought to quash subpoenas issued out of Washington, D.C. that were aimed at their students in Massachusetts. SBC has filed a lawsuit in the Northern District of California seeking to have the entire process declared unconstitutional. Columbia University is also seeking to quash subpoenas that RIAA has attempted to serve on it issued by the District of Columbia courts.[4]

---

[3] Indeed, press accounts indicate that the clerk's office of the district court in D.C. has been overwhelmed with subpoena requests and has been forced to reassign staff from other judicial duties. *See Ted Bridis,* Music Industry Wins Approval of 871 Subpoenas Against Internet Users, Associated Press (July 19, 2003) at 2 ("The RIAA's subpoenas are so prolific that the U.S. District Court in Washington, already suffering staff shortages, has been forced to reassign employees from elsewhere in the clerk's office to help process the paperwork, said Angela Caesar-Mobley, the clerk's operations manager.").

[4] The Federal Rules of Civil Procedure generally provide for the issuance and service of subpoenas in the district where the party in possession of the material resides to protect the rights of third parties to contest the subpoena. *See* Fed. R. Civ. P. 45(a)(2) & 45(b)(2) (placing jurisdictional and service limitations on district court subpoenas for the protection of those from whom production is sought). Despite the fact that Congress expressly provided that the protections of Rule 45 should apply to Section 512(h) subpoenas, *see* 17 U.S.C. § 512(h)(6), RIAA has taken the position that it may obtain and serve a Section 512(h) subpoena from any district court in the country.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00116 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.066

In Verizon's view, Congress never intended to unleash a massive wave of subpoenas on public and private Internet service providers and their customers. This is not an effective solution to the very real problems faced by copyright owners, it only creates an additional level of problems for Internet service providers and chills the free exchange of protected content over the Internet. The use of the subpoena power in an attempt to create an *in terrorem* effect over the entire Internet is both improper and disserves the long-term interests of both copyright owners and Internet service providers. When Congress enacted the DMCA in 1998, it outlined a set of carefully crafted take-down duties for material hosted by service providers. Service provider duties were carefully calibrated to the service providers' involvement with and control over the particular material asserted to be infringing. Congress created a subpoena power to identify only those individuals who were directly linked to specific material residing on the service provider's network that could be "taken down." The language of the of the statute addressing the subpoena power makes three separate cross-references to notices and procedures that only apply in the context of material residing on a service provider's system or network.[5] The subpoena provision was never intended to apply to materials residing on the user's hard drive, such as e-mails, instant messages, or shared files *i.e.*, situations where the ISP is serving in a pure transmission or "conduit" role as described in the statute. By stretching the subpoena power to address a problem that was not before the Congress that enacted the DMCA, the district court has created a Frankenstein monster that Congress never contemplated and that has the potential to cause

(Continued . . .)
Thus, in its view, it could seek a subpoena from the district court in Guam targeting a small service provider in New England.

[5] *See* 17 U.S.C. § 512(h)(2),(4) & (5). Indeed, the statute provides that a subpoena may only issue if "the notification filed satisfies the provisions of subsection (c)(3)(A)," *id.* § 512(h)(4), a provision that only applies in the context of material residing on a service provider's system or network. This limitation makes perfect sense in light of the fact that infringing material available on websites was the principal problem before the Congress that passed the DMCA in 1998.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00117 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.067

irreparable damage to public confidence in the privacy of Internet communications. Given the concerns the Congress expressed throughout the DMCA regarding the protection of the privacy rights of individual Internet users,[6] Verizon submits this is a clear perversion of Congressional intent.

Title II of the DMCA was designed to protect Internet service providers from copyright liability in order to promote the growth of the Internet as a medium of political, social, and economic exchange. But like the telephone itself, that medium depends upon the confidence of users in the privacy of their communications and communications habits. Every person in this room believes that his or her private e-mail or web browsing habits can and should remain private—yet the district court's erroneous decision in the RIAA matter has turned the DMCA into a direct threat to that privacy. It has also burdened Internet service providers with responding to thousands of subpoenas. From our own experience, we can tell you that RIAA's barrage of subpoenas has diverted and strained our internal resources. This new burden on service providers—responding to thousands of subpoenas issued in the conduit context—was never part of the statutory compromise embodied in the DMCA. It also threatens the limited resources of subpoena compliance units to satisfy legitimate law enforcement requests—as RIAA bombards service providers with dozens of subpoenas and purports to require responses on seven days or less notice. The protection of copyright, however legitimate a cause, should

[6] *See* 17 U.S.C. §§ 512(m), 1205. *See also* S. Rep. No. 105-190, at 18 (1998) ("[T]he committee concluded that it was prudent to rule out any scenario in which section 1201 might be relied upon to make it harder, rather than easier, to protect personal privacy on the Internet."). Ironically, the district court's decision in the RIAA case has constituted Section 512(h) as a far greater threat to personal privacy on the Internet than any of the technological copyright protection devices that the Committee was concerned about when it included Section 1205 in Title I of the DMCA.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00118 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.088

never be raised above law enforcement and national security efforts—efforts Verizon has always been in the forefront of supporting and cooperating with.

Both the district court in our case and the copyright owners have eschewed a more measured remedy that has always existed in the law and is used by numerous businesses for many purposes, the so-called "John Doe" lawsuit. Under this procedure, a judge or magistrate reviews the merits of a case before a subpoena is issued, and the defendant is given notice and an opportunity to contest disclosure. The law demands a reasonable investigation of the relevant facts, ownership of a valid copyright registration, and a complaint filed in compliance with Rule 11. Verizon has successfully used this process to sue unknown spammers who abuse our network. Despite the Recording Industry's assertions to the contrary, the filing of a John Doe lawsuit is much more protective of all parties' interests than the DMCA subpoena process.

Since RIAA launched its subpoena campaign, the DC Clerk's Office publicly complained that its internal resources were being burdened and the clerk's office had to re-assign new employees to the fulltime task of processing subpoenas on an ongoing basis. If the district court's decision in our case is not overturned quickly, it threatens to turn the Federal courts into free-floating subpoena mills, unhinged from any pending case or controversy, capable of destroying anonymous Internet communication, and threatening privacy and due process rights as well as public safety.

While Verizon firmly believes that this subpoena process and the tactic of targeting college students, universities, libraries and other individual Internet users is inappropriate and will lead to serious harms with little gain in copyright protection, Verizon recognizes that a more comprehensive and long-term solution is necessary. This Committee should promptly call the interested parties together, to negotiate and establish a balanced process that addresses the

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00119 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.069

legitimate needs of copyright owners while respecting the fundamental due process and privacy rights of Internet users, and recognizing the capabilities and limits of Internet service providers in policing content not under their control. Indeed, this Committee recognized in its report on the DMCA in 1998 that technological rather than legal solutions constituted the best method of ensuring the lawful dissemination of copyrighted works in our new networked, digital environment. *See* S. Rep. No 105-190, at 52 (1998) ("The Committee believes that technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age."). If some form of subpoena power is deemed necessary in conjunction with technological solutions, it must be more limited and contain substantial protections for both ISPs and their subscribers. Any compromise should include, among other requirements, notice to subscribers and an opportunity to defend against such subpoenas, a requirement that all the elements of copyright infringement be established, that the jurisdictional requirements of the federal courts be met, and that a judge approve any subpoena prior to its issuance, as well as penalties for any misuse of the subpoena process, full reimbursement of costs for Internet service providers, immunity for ISPs who provide customer information in response to valid subpoenas, and protection of confidential subscriber data from publication or other misuse. This Committee never had an opportunity to address and balance those interests in 1998 because the technologies at issue simply did not exist. It should do so now before irreparable damage is done to public confidence in the Internet as a medium of free expression and association.

I thank the Chair and the members of this Committee for your attention. We look forward to working with you to resolve this critical issue.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00120 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.070

TESTIMONY OF

MR. ROBBIE CALLAWAY
Chairman

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

On

Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks

For the

U.S. Senate
Judiciary Committee

September 9, 2003

Mr. Chairman and members of the Committee, I am pleased to appear before you today and express the views of the National Center for Missing & Exploited Children regarding the issue of Peer-to-Peer networks as they relate to the distribution of child pornography.

The National Center is intimately involved with the issue of sexual exploitation of children over the Internet, through its Exploited Child Unit and the congressionally mandated CyberTipline – the "911 of the Internet".

The National Center, in partnership with the Federal Bureau of Investigation, Bureau of Immigration and Customs Enforcement, U.S. Secret Service, the U.S. Postal Inspection Service, and state and local law enforcement in Internet Crimes Against Children Task Forces, serves as the Nation's CyberTipline and as the national Child Pornography Tipline. We ask that individuals contact us with information that will help in our fight against child sexual exploitation. The information is forwarded to law enforcement for investigation and review, and, when appropriate, to the Internet service provider. The U.S. Congress has funded these initiatives for reporting child sexual exploitation.

Types of child sexual exploitation that the National Center analyzes include: possession, manufacture, and distribution of child pornography; online enticement of children for sexual acts; child prostitution; child-sex tourism; child sexual molestation (not in the family); and unsolicited obscene material sent to a child.

As of August 24, 2003, the CyberTipline has received over 145,000 reports regarding various types of child sexual exploitation. The CyberTipline has received 1513 reports regarding child pornography being traded by Peer-to-Peer users.

Several of these CyberTipline reports resulted in the arrest of those individuals who were trading sexually explicit images of children. Interestingly, all of these arrests occurred during 2001 and/or early 2002. We did not receive any peer-to-peer reports in years 1998-2000, and the peer-to-peer reports grew five-fold between years 2001 and 2002. According to NCMEC records, there do not appear to be any CyberTipline reports during the last year involving Peer-to-Peer networks that resulted in an arrest. One clear reason exists which explains the reduction in arrests:

In recent years, peer-to-peer programs have been making it more difficult to identify the users. In the past, we were able to easily identify offenders trading child pornography using peer-to-peer programs because their Internet Protocol (IP) addresses were visible and they were required to

93014.072

reveal their email addresses. This is no longer the case. When we receive peer-to-peer reports to the CyberTipline, it is almost impossible to identify the perpetrators responsible for trading the illegal files. The anonymity of recent peer-to-peer technology has allowed individuals who exploit children to trade images and movies featuring the sexual assault of children with very little fear of detection.

It is important to mention that while tracking users trading illegal content on peer-to-peer programs has become increasingly difficult, it is not impossible. Savvy computer users can use certain commands to attain an IP address of a user sending a file. Also, several proactive law enforcement agencies, including Naperville, Illinois's Detective Mike Sullivan, have begun to use secondary programs to identify the IP address of the perpetrator sending the illegal files. However, these programs must be active at the exact moment of file transfer. Depending on the peer-to-peer program, if a user accidentally downloads an illegal file, there is no way for that user to document where the file originated. Considering the massive amounts of files being shared at any given moment, this anonymity provides an incredible cloak of security for those criminals trading images of children being sexually abused.

It is quite likely that the extensive swapping of child pornography images on peer-to-peer networks would reduce if users knew that recipients of the images/movies could easily attain their IP address.

As I stated earlier, the National Center has received leads on over 1500 peer-to-peer trades of child pornography. I'd like to now demonstrate the National Center's involvement in two cases where there was a successful resolution from peer-to-peer CyberTipline reports:

On April 19, 2001 the CyberTipline received an anonymous complaint regarding child pornography being traded on a peer-to-peer network. During his searches, the caller found a disturbing image that he described as, "two little girls touching themselves below the waist." According to the caller, the girls appeared to be approximately 12 years of age.

NCMEC analysts conducted a search of the peer-to-peer network and found numerous images of child pornography being traded. One individual trading these images was using an IP address registered to the University of California – Santa Barbara. NCMEC contacted UCSB Campus Police.

Subsequently, university detectives, working with the Santa Barbara Sheriff's Department High-Tech Crime Unit, were able to verify the existence and location of the offender. A 21-year old suspect was identified and a search warrant was executed at his apartment located off

93014.073

campus. A forensic search of his computer found numerous child pornography images. The suspect confessed and the District Attorney's Office filed felony charges of distributing child pornography on May 17, 2001.

On May 20, 2002, the National Center received a CyberTipline report referring to a suspect who was trading child pornography through a peer-to-peer program. This reporting person was highly skilled with computers and used commands to document the IP address of the person trading the child pornography images. Using detailed information provided by the reporting person, it was determined that the suspect had connected to the Internet from Manhattan, Kansas.

The National Center contacted law enforcement officials in Kansas and provided them with the documentation of the illegal files being traded from their jurisdiction. The police apprehended the suspect and charged him with 500 counts of possession/distribution of child pornographic material, sexual exploitation of a child, and indecent liberties with a child involving his own. The suspect admitted to raping, sodomizing and sexually abusing his daughter.

It is unlikely this predator would have been arrested if a concerned citizen hadn't known the correct steps to take when she accidentally received one of his images. It is troublesome to imagine the number of offenders who are not reported because the average citizen does not know how to collect the necessary information. Peer-to-peer program developers could make great strides in protecting children if they allowed software programs to allow users to log the origination of files.

A decade ago, FBI Special Agent Ken Lanning, now retired, author of NCMEC's major publications in this field, outlined for Congress why pedophiles collect and distribute child pornography:

1. To justify their obsession for children
2. To stimulate their sexual drive
3. To lower a child's inhibitions
4. To preserve a child's youth
5. To blackmail
6. As a medium of exchange
7. For profit

As Agent Lanning noted, molesters use child pornography to stimulate their own desires and fuel their fantasies for children as sexual partners. Viewing these images whets the appetite of the molester and serves as a precursor to his own sexual acts with children. The more frequently a molester views child pornography, the more he, like his child victims,

93014.074

becomes desensitized to the abnormality of his conduct. He can convince himself that his behavior is normal, and eventually he will need more and increasingly explicit child pornography to satisfy his cravings. When mere visual stimulation no longer satisfies him, he will often progress to sexually molesting live children.

There is compelling evidence that child pornography will cause real physical, emotional and psychological damage not only to those children involved in the pornography, but potentially to children who are shown that child pornography, and who are lured into performing sexual acts because of the reasons that Agent Lanning states, including lowering their inhibitions.

We will all agree that children who are involved in child pornography are, by the very nature of the industry, victims of sexual exploitation and sexual abuse. Ann Wolbert Burgess, of the Boston College Nursing School, states, "The destructive effects of child sexual abuse can create a number of long-term problems for the child victim. Studies of sexually exploited children indicate a variety of long-term emotional, behavioral, social, and sexual problems. Symptoms include physical problems of headaches, stomachaches, and sleeping and eating disorders; psychological reactions of fear and anxiety, depression, mood changes, guilt, and shame; social problems of school truancy, declining grades, and fighting; and sexual problems, such as heightened sexual activity, compulsive masturbation, exhibitionism, and preoccupation with sex and nudity. Running away from home, adolescent prostitution, suicide attempts, substance abuse, gender identity confusion, sexual dysfunction, and socially deviant behaviors have also been identified as possible consequences of untreated childhood sexual abuse."

To summarize, the National Center believes the use of peer-to-peer networks for the distribution of child pornography is a growing problem. We suspect that there is an increase in distribution as pornographers look for lower risk avenues where the possibility of being identified is less. Law enforcement faces numerous challenges including:

- There is no central database of files nor organized network
- There are no centrally-held logs on these systems to record activity
- Most of the popular file-sharing programs are free so there is no subscriber information available upon subpoena to determine the user's true identity
- These are dynamic systems where content and users change very rapidly. This often requires law enforcement officers to be online at the moment the offense occurs.
- Individuals from all over the world use these peer-to-peer programs.

93014.075

The National Center's CyberTipline is the nation's primary vehicle for reporting sexual exploitation of children, and we would be interested in playing an even larger role than we currently do.

I don't have an answer today on how to combat the all-pervasive problem of trading illegal child pornography on the Internet, but I thank you, Mr. Chairman, for calling this hearing to order to begin dialogue on this problem. We look forward to continuing a discussion and analysis of distribution of child pornography on the Internet via peer-to-peer networks.

93014.076

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 8, 2004

The Honorable Patrick J. Leahy
Ranking Minority Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Leahy:

This letter is in response to your letters of September 3, 2003, October 10, 2003, and March 8, 2004, to the Attorney General. In your letters, you asked for the views of the Department of Justice (the "Department") regarding whether 42 U.S.C. § 13032 (the "Statute") is applicable to Internet Peer-to-Peer (P2P) networks. You also reiterated your concern that the Department has not yet issued regulations implementing the Statute.

In response to the first issue, the term "network" in the P2P context generally does not connote a central authority with oversight over file sharing transactions, but rather, simply means a series of individual computers sharing files with one another at any given moment. As a result, it is unclear whether the distributors of the software that allows individuals to share files on their computers (such as KaZaA) have any specific knowledge of, involvement in, or control over this activity. So far as the Department is aware, these software distributors do not provide "electronic communications services" or "remote computing services" as those terms are statutorily defined, *see* 18 U.S.C. §§ 2510(15), 2711(2), and, therefore, do not fall within the mandate of the Statute. Moreover, even if P2P software were technologically capable of allowing its manufacturers to monitor the activities of their users, and even if the manufacturers qualified as providers of electronic communications services or remote computing services, the Statute specifically states that providers have no duty to monitor the content of their users' communications. *See* 42 U.S.C. § 13032(e).

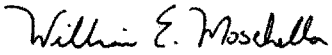
In that the "networks" in the P2P context generally consist of ordinary citizens trading files, those individuals also do not fall within the mandatory reporting statute. Nevertheless, citizens do report the presence of child pornography on the Internet to the National Center for Missing and Exploited Children's ("NCMEC's") Cyber Tipline, though this is purely voluntary.

The Honorable Patrick J. Leahy
Page 2

In regard to the second issue that you raise, the Attorney General is authorized to designate the law enforcement agencies to which reports may be forwarded by NCMEC, but the statute does not authorize implementing regulations to impose duties on Internet service providers ("ISPs"). *See* 42 U.S.C. § 13032(b)(2). Accordingly, the regulations can suggest, but not require, that ISPs report suspected violations in specific ways. The vast majority of large ISPs with whom the Department has consulted have indicated a desire to implement reporting in the manner most useful to NCMEC and the law enforcement community. The Department has been working with NCMEC, the Federal Bureau of Investigation, the Department of Homeland Security's Bureau of Immigration and Customs Enforcement, the United States Secret Service, the United States Postal Inspection Service, and the major ISPs to achieve consensus on the reporting protocols. This is a time-consuming process, particularly because of the technical constraints of both the individual ISPs and NCMEC, that necessarily dictate the limits of any reporting protocol. The Attorney General published the initial designation of four law enforcement agencies to which NCMEC should forward reports on November 4, 2003. *See* 28 C.F.R. 81.11 *et seq*. As the Department gathers a consensus on a more comprehensive set of guidelines both for IPSs reporting to NCMEC and for NCMEC's reports to law enforcement, the Department will publish these operating guidelines. The Department appreciates the support of the ISPs in this endeavor and expects to be able to develop a consensus protocol.

We trust that this information is helpful to you. Please feel free to call upon us if we may be of additional assistance.

Sincerely,



William E. Moschella
Assistant Attorney General

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00128 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.078

Statement
United States Senate Committee on the Judiciary
"Pornography, Technology, and Process: Problems and
September 9, 2003

The Honorable Orrin Hatch
United States Senator , Utah

Statement of Chairman Orrin G. Hatch

Before the United States Senate Committee on the Judiciary

Hearing on

"Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks"

In this hearing we continue our examination of an explosively popular and promising technology, which counts among its users millions and millions of teens and pre-teens worldwide: peer-to-peer file sharing networks.

At our last hearing on peer-to-peer networks, we examined some of the personal and institutional security risks associated with P2P usage. Today's hearing focuses on a different set of issues – and the questions they raise – that are equally pressing.

The first panel will address an issue that is very deeply disturbing to me, and I know to other lawmakers as well: the presence on peer-to-peer networks of enormous quantities of pornographic materials, including child pornography, and the great risk of inadvertent exposure to these materials by young P2P users. This is an issue of critical importance to parents, who must be educated about these risks and equipped to control or eliminate them.

The second panel will address the information subpoena provisions of the Digital Millennium Copyright Act, and I will have more to say about that issue after we hear from our first panel.

I know that we here in Congress, along with all upstanding Americans, agree on this: Child pornography is inherently repulsive, inherently victimizing, and intolerable in any form. It is both an effect and cause of sickness: perverts and pedophiles not only use child pornography to whet their

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00129 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.079

sick desires, but also to lure our defenseless children into unspeakable acts of sexual exploitation.

My commitment, Senator Leahy's commitment and this Congress' commitment to eradicating child pornography was evident in the passage of the PROTECT Act, which Senator Leahy and I co-sponsored.

As we are about to hear, peer-to-peer networks provide a new and growing means for distribution of these disgraceful materials. They also pose unique challenges for law enforcement trying to combat child pornography and unique and unacceptable dangers to our children.

The following video presentation conveys the depth and urgency of these dangers. So I would like to complete my opening remarks with a showing of this video, which was produced by the RIAA, in collaboration with the Suffolk County, New York District Attorneys Office, which is represented here today, the Los Angeles Council on Child Abuse and Neglect, and Media Defender, a security company that has testified repeatedly before Congress and this Committee.

I should warn you that some of the language in this video is graphic, and the content is disturbing, but this is what our children are witnessing on peer-to-peer networks and we need to know about it. An edited transcript will be prepared for the record.

VIDEO PRESENTATION

Our second panel will address the ISP-subpoena provisions of the Digital Millennium Copyright Act, a critical part of a compromise that this Committee helped negotiate between the content and technology industries. This compromise was intended to permit both the development of Internet services and the enforcement of copyrights on the Internet.

This compromise is now codified in Section 512 of the Copyright Act. Section 512 creates so-called safe-harbor provisions that protect Internet service providers from secondary liability for copyright infringement. These safe-harbors protect ISPs regardless of whether their systems act as conduits, locators or hosts for infringing materials posted by third parties.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00130 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.080

In exchange for these safe-harbors, Section 512 requires ISPs to provide specific assistance to content creators alleging that someone is using ISP services or systems to host, locate, or transmit infringing content. For example, Section 512 can require an ISP to remove allegedly infringing materials hosted by the ISP or to identify an allegedly infringing customer in response to a subpoena under Section 512 (h). Recently, the subpoena provisions of Section 512(h) came under scrutiny when they were invoked by content creators trying to identify individuals allegedly trading infringing materials over peer-to-peer file-sharing networks.

Our second panel consists of three panelists who will discuss the legal and policy implications of the subpoena provisions that underlie both the Section 512 compromise and our broader system for reconciling copyright and the Internet. Mr. Cary Sherman is the President of the Recording Industry Association of America; his organization has served Section 512(h) subpoenas to obtain identifying information about individuals alleged to have trading infringing music files over peer-to-peer file-sharing networks. Mr. William Barr is the General Counsel of Verizon; his company provides ISP services and has received Section 512(h) subpoenas. Our last panelist, Ms. Marybeth Peters, is the Register of Copyrights; she brings to this narrow but important dispute about Section 512(h) subpoenas her unquestioned expertise with the broader issues of law and policy that underlie both the DMCA and the Copyright Act. She as also been gracious enough to help us streamline this large hearing by agreeing to appear on the same panel as our private-party witnesses and agreeing to go last in order to provide some perspective on the views of the two preceding litigants.

###

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00131 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.081

University of Utah
Peer-to-Peer File Sharing

Stephen Hess
Associate Academic Vice President for Information Technology
Office of Information Technology
University of Utah

September 9, 2003

Overview

The University of Utah is the oldest university west of the Mississippi, offering 75 undergraduate degree programs, along with more than 38 teaching majors and minors, and over 90 graduate majors. The University is ranked among the top 35 research institutions in the nation with particular distinction in medicine, genetics, and engineering.

2002 Fall Semester enrollment was 28,000. Of these, 86% are "resident" students. 44% of the "non-resident" population consists of international students. Less than 1% of the students live on campus in apartments and dormitory facilities.

Importance of Information Technology and Networks

The University of Utah was one of four original pioneers of the ARPANET education and research network (1969) which became the Internet we know today. The University continues to be a leader in the development and delivery of networked electronic services to its constituents.

The University of Utah is home to the Utah Education Network (UEN) which provides electronically delivered educational resources *and Internet connectivity to all of Utah's institutions of higher learning, school districts, and public libraries*. The UEN provides statewide coordination of distance learning for public and higher education, including Utah's Electronic High School and Electronic College.

The successful fulfillment of the higher education and public education mission is inextricably tied to internal networks, computing resources, and the Internet.

Peer-to-Peer – An Evolving Technology

The University can foresee the emergence of a wide range of collaborative, project management, business planning, and academic/educational applications, that could take advantage of the underlying technical architecture of Peer-to-Peer technologies.

A few developing applications have begun to demonstrate the power of Peer-to-Peer communications. These emerging applications when combined with other Peer-to-Peer collaboration tools, such as Instant Messenger, may enhance an individual's academic experience and expand educational opportunities to more citizens.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00132 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.082

Groove Networks, Microsoft, Apple, and other software vendors appear to be poised to launch a new wave of interest in Peer-to-Peer. These new applications may enable individuals to collaborate with each other, to participate in audio and video conversations, and to exchange files and information. One can easily imagine the business, government and education applications that may be enhanced by these developments. [i]

Peer-to-Peer (P2P) services have been controversial since their inception. Tens of millions of users freely share music, movies and software. The entertainment and software industries have increased their efforts to prevent sharing of copyrighted materials. Businesses and organizations like the University of Utah, which own networks and act as Internet service providers to their constituents, have been caught in the middle of this struggle.

With the rise of Napster, universities scrambled to find a way to block or restrict P2P activity. At first, this was relatively easy and only required a simple port block at a router. Products like Morpheus and Kazaa emerged and became the preferred service for quick and easy downloads. At first, these could be easily blocked.

In early versions of P2P software, a network administrator was able to use a simple command to connect to a P2P client, and obtain a list of content being shared from that computer. The privacy of the individual was not an issue because the person offering downloads was *publicly* posting their content.

Then Kazaa version 2 arrived. This clever "upgrade" in P2P software removed the ability to view content with simple connections, and added basic firewall evasion tactics. The new version also allowed anyone sharing files to be classified, or "promoted" to a "Super-Node" status, depending on the quality of the network to which they are connected. The P2P client software literally promotes itself, based on how much bandwidth is available to it, moving the computer higher on the list of desirable download sites. This has been a significant change for higher education institutions because of their high speed Internet connections. [ii]

When the Recording Industry recently announced that it would more aggressively pursue legal remedies against those who share copyrighted materials, Peer-to-Peer usage decreased somewhat. However, software developers have indicated their intent to alter P2P software to mask the identities of file sharers.

The use of Peer-to-Peer file sharing to introduce malicious code (virus and worms) is also a growing problem. The time may be approaching when the total risk of operating a Peer-to-Peer software sharing client on a network outweighs even the needs for legitimate uses of this technology. [iii]

These issues place universities in a very difficult position, trying to find a balance between enabling a promising new technology, while discouraging inappropriate, illegal, or threatening behavior.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00133 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.083

In an effort to resolve this dilemma, a Joint Committee of the Higher Education and Entertainment Communities was formed last fall and is comprised of leaders representing universities, higher education organizations, and music and motion picture executives. The committee aims to provide a range of resources to school administrators in three basic areas: educational efforts (including practices surrounding the use of copyrighted works, student responsibility, and implications for peer-to-peer network file sharing), technological solutions (including computer network management technologies available to reduce illegal file sharing and the development of legal, campus-based music and movie/entertainment services), and examining differences and exploring prospects for collaboration on legislative initiatives.

What is the University of Utah's stance on Peer-to-Peer file sharing?

The University deals with Peer-to-Peer file sharing based on compliance with State and Federal laws and regulations and University policies governing the appropriate and acceptable use of information resources.

The University considers the illegal sharing of copyrighted materials a violation of the U.S. Copyright Act. The University's acceptable use policy is also violated when any of the following occur:

1. The behavior is not a valid educational or academic activity.
2. The behavior is not required to conduct the business of the University.
3. The behavior does not show restraint in the utilization of shared resources.
4. The behavior is not consistent with intellectual property rights and/or ownership of data.
5. The behavior compromises the security of information resources.
6. The behavior monopolizes resources or reduces other's access to information resources.
7. The behavior wastes University resources.
8. The behavior results in illegal copying, storing or transmitting of patented or copyrighted materials using University resources.
9. The behavior violates any federal or state laws, including copyright, pornography, or export laws.

What steps does the University of Utah take to monitor its network?

The University of Utah, like other institutions of higher education, places a high value on academic freedom and inquiry and the free flow of information of all types with a reasonable expectation of privacy. Therefore, the University monitors traffic flows, not content. *Traffic*

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00134 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.084

flow is a measure of the amount of data that is transmitted over a network, while *content* is the information contained within the data flow.

The Utah Education Network serves public education (K-12) and libraries and therefore does provide content filtering services for those entities that need to screen content that is inappropriate for the consumption of minors.

The primary purpose of data flow monitoring is to identify patterns of network activity that may affect the health and availability of network resources. Suspect flow patterns include unusually high bandwidth consumption which may, or may not indicate Peer-to-Peer file sharing activity.

The University's acceptable use policy allows content monitoring only for the purpose of evaluating an employee's job performance. All monitoring must be relevant to work performance. Employees receive information about their work that is gained through monitoring. Disclosure and use of resulting data is restricted to University-related purposes.

For example, if an employee's job performance is declining, and it is suspected that the reason is that the employee's time is being used for non-job related Internet activity, the Supervisor, with approval of the appropriate Vice President, may request that the employee's network use be monitored. The employee is informed that their use of the network will be monitored before the monitoring actually occurs. Employees typically discontinue the inappropriate use of the network when they receive notice that monitoring will occur. If inappropriate use continues, the employee is subject to disciplinary action in accordance with University policy.

The University also collects "top talker" reports. These reports identify networked devices that use the highest percentage of available bandwidth. Because the University must maintain its network and plan for future demand, we inquire as to the actual use of "top talking" users. Student housing residents, who appear on a "top talker" report, usually acknowledge downloading or sharing large amounts of P2P data. However, not all users that are sharing copyrighted materials appear on a "top talker" report. [iv]

The University may disconnect "top talkers" who share copyrighted materials over Peer-to-Peer networks once we are aware of it.

These steps have been effective in reducing illegal Peer-to-Peer file sharing.

What is the University of Utah's experience with Peer-to-Peer file sharing?

During periods of high Peer-to-Peer activity, i.e., when students return in the fall, P2P traffic may total as much as 30% of the total bandwidth consumption. Without active management, it is possible for the top ten "top talkers" to monopolize as much as 15% of the University's bandwidth.

Peer-to-Peer file sharing impacts educational networks operationally *and* economically. File sharing can slow networks, restrict access for legitimate academic pursuits, and require the acquisition of more bandwidth to meet legitimate academic requirements.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00135 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.085

What is the University of Utah doing about Peer-to-Peer file sharing?

Education is an important key to resolving file sharing issues. The open nature of the Internet has led people to believe that virtually anything found on the Internet is free for the taking. Internet users must learn that principals of ethical and appropriate behavior on the net should not differ from expected behavior in life outside of the Internet.

New students receive instruction regarding Peer-to-Peer file sharing during new student orientation sessions. E-mail and web sites are used to communicate with faculty, staff, and students regarding Peer-to-Peer file sharing.

The processes and procedures used by the University to deal with specific copyright violations and inappropriate P2P file sharing include the following.

1. Receipt of Notification. The copyright holder notifies the University of an allegation of copyright infringement and requests that the University take action to remedy the situation.

2. Discontinuation of Service. The University immediately disconnects the computer alleged to be illegally uploading or downloading copyrighted materials and deactivates the user ID of the individual responsible for that computer.

3. Teaching Opportunities. Service is not restored until the user meets with the University's Security Office so that the complaint can be fully investigated. Depending on the findings, the student is instructed regarding the consequences of illegal file sharing and signs an agreement, stating that they will cease all such activity. The end user is informed that signing the agreement does not release them from the possibility of further liability under the U.S. Copyright Act.

4. Proactive measures. "Top talkers" are contacted. If illegal file sharing is disclosed or discovered, the responsible party receives the same treatment as someone who is the subject of a complaint from the entertainment or software industry.

5. Technology vs. Technology. The University has made attempts to block inappropriate file sharing using technological solutions. However, these solutions have not been successful, in spite of the abilities of extremely talented information technology professionals.

    a. Blocking router ports. File sharing software evolves as fast as a network administrator can make such changes, making this an expensive and ineffective solution.

    b. Rate-limiting or "shaping" bandwidth. This entails limiting the amount of bandwidth that is available to end users. When this approach is used, appropriate academic uses may also be restricted.

    c. Access Control Lists to prevent Peer-to-Peer sessions. This solution invariably restricts legitimate network uses and is therefore unacceptable.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00136 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.086

While these procedures do not prevent new incidents of P2P file sharing, the University has been able to virtually eliminate the incidence of repeat offenses.

Pornography

While the University does not monitor content of network transmissions in the normal course of business, this does not mean that downloading pornographic materials using Peer-to-Peer networks, or storing such information on University owned computing devices is an acceptable use of University resources.

Provided that the use of pornography is not for academic or research purposes, this behavior is dealt with in terms of job performance and is handled through the supervisor/employee relationship. If a person is using work hours to download or view pornography, shop on e-bay, play games, or is using the network for any other excessive, non-incidental, performance impacting personal activity, they are subject to University acceptable use and employment policies.

At times, computers in student laboratories have been used to view pornography or for other non-academic pursuits. This activity is typically discovered by the lab staff, sometimes by receiving a complaint from another lab patron. The University's experience indicates that most of this behavior does not involve, faculty, staff, or faculty members, but rather, is the result of walk-in traffic into open access laboratories, i.e., campus library computing labs. This problem is diminished, almost entirely, when access to the network requires the user to authenticate, or log onto the network, using a distinctive user ID and password.

In the event that a student, faculty member or staff member is found to possess illegal pornography, i.e., child pornography, whether or not it was downloaded from the Internet and stored on University information technology resources, they are deemed to be in violation of federal and state laws and are reported to the appropriate law enforcement agencies.

---

[i] Barry Bryson, Associate Director Technical Operations, Utah Education Network
[ii] "A Conversation on Peer-to-Peer," Troy Jessup, Network Security Professional, Utah Education Network, http://www.ndnn.org/blog/archives/000071.html
[iii] "A Conversation on Peer-to-Peer," Troy Jessup, Network Security Professional, Utah Education Network, http://www.ndnn.org/blog/archives/000071.html
[iv] Rhett Jones (Jonzy), IT Security Professional, Institutional Security Office, University of Utah

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00137 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.087

Testimony
United State Senate Committee on the Judiciary
Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks

September 9, 2003

Dr. Doug Jacobson
Associate Professor, Electrical and Computer Engineering, Iowa State University
President & Chief Technology Officer, Palisade Systems, Inc.

Mr. Chairman and members of the committee I would like to thank you for the opportunity to appear before you today to discuss the issues surrounding peer-to-peer networks.

By way of introduction, I wear several hats. I'm currently an associate professor of Electrical and Computer Engineering at Iowa State University. My duties include teaching advanced network protocols and a course on information warfare. I also serve as the Director of Iowa State's Information Assurance Center, which has over 30 faculty associates on campus. Iowa State University was one of the first seven universities designated a Center of Academic Excellence in Information Assurance Education by the National Security Agency. For the past seven years I have assisted local law enforcement agencies in investigating numerous computer crimes including software theft, harassment, and child pornography.

I also started a security and Internet filtering company in 1996 and currently serve as its president and chief technology officer. Palisade Systems was formed to address the issue of pornography on school networks. The patented technology licensed from Iowa State University enabled Palisade Systems to develop its first product called ScreenDoor, which is a web filter. In summer of 2000 we introduced PacketHound which is designed to detect, monitor, and block unauthorized peer-to-peer applications. This product was so unique that it won an R&D 100 award in 2001, an honor reserved for the top technology innovations of a given year. Since that time Palisade Systems has become a leader in peer-to-peer technology, conducting research and publishing studies on the subject.

During my testimony today I will discuss the use of peer-to-peer applications for the distribution of pornography. I will talk about how peer-to-peer applications have evolved to challenge the efforts of security professionals to stop their misuse for criminal purposes. Finally I will address the current state of technology used to monitor or block peer-to-peer applications.

First, I would like to address the issue of pornography and peer-to-peer networks. There are several issues that make pornography on peer-to-peer networks more problematic than web or FTP-hosted pornography. You don't have to look for pornography on peer-to-peer networks; it will find you. There are no effective controls regarding content provided on a peer-to-peer network, the only information you are given is a file name. A

93014.088

good example of this problem hit home this spring when I was teaching my information warfare class. To give students an opportunity to study the security problems associated with peer-to-peer networks, I set up a peer-to-peer node. I searched for a file that I had created and placed on the peer-to-peer network. I received several matches to my search request, but when I downloaded and viewed the files, they contained embedded links to pornography sites. It turns out that people have designed custom applications that will answer any query on a peer-to-peer network and return a match to the search string. When the unsuspecting user requests the file, the custom software will return a file containing the embedded links.

Another issue is that peer-to-peer networks seem safer to someone who does not want to be discovered. A user simply types in a search string and receives a list of files that match words in the search string. The user then clicks on the file name and that file is transferred to his or her hard drive. This gives the user a feeling of anonymity. Moreover, this feeling of anonymity works both ways in that the both the provider and the requester of the file are not easily identified and therefore they may believe that their act cannot be monitored.

It is easier to search for pornographic files whose titles contain key words on a peer-to-peer network than to use a standard web search engine. For example, I entered the search string "Teen Sex" into Google and received over 5 million hits, ranging from websites that indicated they contained graphic images to others devoted to discussions of teen pregnancy and other legitimate health and social issues. By contrast, upon entering the same search string into a Gnutella peer-to-peer network, after one minute I received a far more narrow listing of more than 1300 matches containing *only* movies and pictures whose names implied specifically pornographic content, including a number of sources offering access to child pornography. A quick review of both lists showed that the peer-to-peer network provided a quicker and easier way to obtain pornography of all varieties.

Palisade Systems conducted a study of searches on a Gnutella network. Acting as a node on the network, we gathered 22 million searches between February 6 and February 23, 2003. Details identifying the individual such as the IP addresses were removed to maintain the privacy of the users. In addition, none of the requested files were downloaded.

Over the nearly three weeks of monitoring, the study found that:

- 42% of all requests were for all types of pornography (168,000 of 400,000 search requests)
- 6% of all search requests were specifically for child pornography (24,000 of 400,000 search requests)

While this study focused on search requests you could reasonably assume that the number of hits would be proportional to the number of requests, since people don't constantly search for things that they can't find. Studies published by other organizations

93014.089

have come to similar conclusions all backing the claim that peer-to-peer networks have become a widely accepted vehicle for the distribution of pornography.

Palisade Systems has been monitoring peer-to-peer networks on an on-going basis since the conclusion of the first study. Although I am not able to release statistics, we have gathered significant examples of pornography being downloaded at federal and local government agencies and elementary schools across the nation. There are two or three other companies that can also provide similar information. We will be reporting our findings in a report within the next month.

Many articles have been published about the more dangerous uses of peer-to-peer applications, ranging from security violations to child pornography. I would like to focus briefly on the methodology used by peer-to-peer applications to avoid detection and to hide both the content and the source of the information. An argument could be made that, other than for governmental security purposes or to protect the transfer of confidential or proprietary information between commercial interests, legitimate peer-to-peer applications would not need to hide from detection or evade monitoring.

Information sharing on the Internet has moved from a centralized approach with FTP servers, WAREZ sites, and web servers to a distributed approach. For those of you unfamiliar with them, a WAREZ site is used to store and distribute pirated software or other illegal information. In some measure, this transition has been a reaction to the successful efforts of system administrators and law enforcement agencies in stopping centralized approaches to illegal file sharing. With a centralized approach there needs to be someone in charge of the system and therefore, an identifiable person who can be prosecuted. However, several new peer-to-peer protocols have been designed to evade detection and to circumvent standard security mechanisms developed to address centralized approaches. While you can argue that peer-to-peer represents a new paradigm in networking and has legitimate uses, a case can be made that certain protocols have been designed expressly to aid in the covert procurement and/or distribution of information. Indeed the reason Palisade Systems developed PacketHound in the first place was because many of these new applications claimed they could not be blocked, thus suggesting a high likelihood of criminal intent.

First a little background. In order for applications to communicate with each other, they need to know two things; they need to know the address of the computer that hosts the application and the address of the specific application. The address of the computer is known as the "IP address" and the address of the application is called the "port number". To use a familiar model, the address of a computer is analogous to the address of house, and the address of the application is analogous to the name of a particular person in that house. Of course, this is how mail can be delivered to the right person at the right house. Similarly, with computer applications you need to know the port number of the application you wish to communicate with. In most cases the port number has been assigned to a given application; for example the World Wide Web is port 80 and email is port 25. From a security standpoint, such an assignment is also helpful insofar as you can

93014.090

stop all traffic directed toward a given set of applications. To use out postal model once more, this would be like tossing all mail addressed to "Occupant."

Peer-to-peer has become the latest battlefield in which developers of peer-to-peer applications are constantly working to outsmart the defenders of the network. I would now like to talk briefly about the state of technology used to monitor, control, or block Peer-to-peer networks. I have chosen to divide the technology into four categories.

The first category is port blocking, which is a common method used at the front end of most corporate networks Early peer-to-peer networks evolved to employ techniques that bypass port blocking mechanisms. The first method was "port hopping", in which the port number is not fixed but can be changed. This approach prevents network administrators from blocking the particular ports associated with the peer-to-peer applications. As administrators adapted and started filtering out all but a few critical ports, peer-to-peer protocols adopted a new technique called "tunneling". In this technique, peer-to-peer protocols used the port number assigned to other applications like web traffic so that their traffic is allowed to pass through the defenses.

Another method is called "signature based," which is the concept behind the Palisade Systems PacketHound product. This technology examines all of the packets on the network to determine if certain patterns (called signatures) can be found on the network. For example, Gnutella always starts a new connection with a certain set of messages. Signature-based technologies require updating whenever a new protocol is found or a current protocol changes. PacketHound can currently detect over 20 Peer-to-peer protocols and has signatures for over 100 protocols.

The "content-based" method involves trying to determine the content of the file being transferred by looking at the data. This technology has had limited success in the web filtering market. We have all heard about web filters blocking access to a website dedicated to cancer research because the word "breast" is contained on some of the pages. This method can work to identify known data like copyrighted music, but does not work when the data is not known or cataloged. For example, there is not a catalog of all known pornographic images therefore a content-based identification could not be used. Palisade Systems has teamed up with a company called Audible Magic to create a product that indicates when peer-to-peer networks are exchanging copyrighted music. Another drawback to content-based filtering is the use of encryption by some peer-to-peer networks.

The final technology is to allow only known traffic types on a network and to block all unknown traffic. This type is often called "white listing" where only the know traffic is allow to pass. This technology can work well in a controlled environment where the traffic is known. Palisade Systems has introduced a product called FireBlock designed to allow only know traffic, which also won the R&D 100 award this year.

The newest steps in the evolution of peer-too-peer networks are "encryption" and "anonymous access". Anonymous access is designed to hide the source of the

93014.091

information. First generation peer-to-peer protocols provided the address of the computer originally containing the file that was downloaded, thus allowing network administrators and law enforcement agencies to trace the source of the files. The latest step in the evolution of peer-to-peer applications uses encryption techniques to hide both the source of the data and the data itself. The best example of this evolution is the newest application called Earthstation 5. This protocol uses encryption, anonymous access, and tunneling. The web site for Earthstation 5 makes it clear they are working to stop any efforts at filtering.

A couple of observations can be made from a review of these technologies. First, while each technology has certain limitations, using multiple technologies in a layered approach seems like the best defense in a corporate environment. However, this method often required knowledgeable staff and constant monitoring of the networks. Second, most technologies are focused on a corporate market. Many of the solutions are cost prohibitive for small organizations like schools, small business, etc. Furthermore, these technologies are not designed for the home users. This leaves individuals on their own to solve the problems of peer-to-peer networking, which naturally leads us to the question "What's the home owner to do?"

Peer-to-peer applications are easy to find and install. If a home user allows these applications to be installed, little can be done to prevent downloading of pornography or other material. Unlike web filtering where certain sites can be blocked and web access can be monitored, peer-to-peer traffic cannot be filtered based on its content. This leaves a home user no choice but to either allow peer-to-peer activity and all of its associated risks or not allow any peer-to-peer applications on their machines.

It would be possible for Internet service providers to offer a service that blocks peer-to-peer traffic similar to the web filtering provided. The bottom line is that the home user needs to be educated about the potential dangers of peer-to-peer networking.

In summary, I've outlined how peer-to-peer networking has evolved to avoid detection and filtering. I see no signs of this evolutionary path slowing down in fact with the advent of the newest protocols like Earthstation 5, we will be facing increasing challenges in the years ahead. Also, given the inherent distributed nature of peer-to-peer protocols and the difficulty in identifying these networks, I predict that peer-to-peer networks will become a method of choice to distribute illegal materials across the internet. Companies like Palisade Systems in conjunction with research universities like Iowa State University will continue to develop new technologies to combat the evolution of peer-to-peer networks.

I would like to thank you for this opportunity to testify today. I would be pleased to answer any questions you might have.

United States General Accounting Office

GAO

Testimony
Before the Committee on the Judiciary, United States Senate

For Release on Delivery
Expected at 2 p.m. EDT
on Tuesday
September 9, 2003

FILE-SHARING PROGRAMS

Users of Peer-to-Peer Networks Can Readily Access Child Pornography

Statement of Linda D. Koontz
Director, Information Management Issues

GAO-03-1115T

93014.093

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

September 9, 2003

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-03-1115T, a testimony before the Committee on the Judiciary, United States Senate

FILE-SHARING PROGRAMS

Users of Peer-to-Peer Networks Can Readily Access Child Pornography

Why GAO Did This Study

The availability of child pornography has dramatically increased in recent years as it has migrated from printed material to the World Wide Web, becoming accessible through Web sites, chat rooms, newsgroups, and now the increasingly popular peer-to-peer file sharing programs. These programs enable direct communication between users, allowing users to access each other's files and share digital music, images, and video.

GAO was requested to determine the ease of access to child pornography on peer-to-peer networks; the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography; and the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks. Today's testimony is based on GAO's report on the results of that work (GAO-03-351).

Because child pornography cannot be accessed legally other than by law enforcement agencies, GAO worked with the Customs Cyber-Smuggling Center in performing searches: Customs downloaded and analyzed image files, and GAO performed analyses based on keywords and file names only.

http://www.gao.gov/cgi-bin/getrpt?GAO-03-1115T

To view the full testimony, click on the link above.
For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

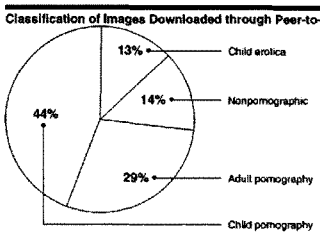
What GAO Found

Child pornography is easily found and downloaded from peer-to-peer networks. In one search, using 12 keywords known to be associated with child pornography on the Internet, GAO identified 1,286 titles and file names, determining that 543 (about 42 percent) were associated with child pornography images. Of the remaining, 34 percent were classified as adult pornography and 24 percent as nonpornographic. In another search using three keywords, a Customs analyst downloaded 341 images, of which 149 (about 44 percent) contained child pornography (see the figure below). These results are in accord with increased reports of child pornography on peer-to-peer networks; since it began tracking these in 2001, the National Center for Missing and Exploited Children has seen a fourfold increase—from 156 in 2001 to 757 in 2002. Although the numbers are as yet small by comparison to those for other sources (26,759 reports of child pornography on Web sites in 2002), the increase is significant.

Juvenile users of peer-to-peer networks are at significant risk of inadvertent exposure to pornography, including child pornography. Searches on innocuous keywords likely to be used by juveniles (such as names of cartoon characters or celebrities) produced a high proportion of pornographic images: in our searches, the retrieved images included adult pornography (34 percent), cartoon pornography (14 percent), child erotica (7 percent), and child pornography (1 percent).

While federal law enforcement agencies—including the FBI, Justice's Child Exploitation and Obscenity Section, and Customs—are devoting resources to combating child exploitation and child pornography in general, these agencies do not track the resources dedicated to specific technologies used to access and download child pornography on the Internet. Therefore, GAO was unable to quantify the resources devoted to investigating cases on peer-to-peer networks. According to law enforcement officials, however, as tips concerning child pornography on peer-to-peer networks escalate, law enforcement resources are increasingly being focused on this area.

Classification of Images Downloaded through Peer-to-Peer File-Sharing Program



Source: Customs CyberSmuggling Center.

United States General Accounting Office

Mr. Chairman and Members of the Committee:

Thank you for inviting us to discuss our work on the availability of child pornography on peer-to-peer networks.[1]

In recent years, child pornography has become increasingly available as it has migrated from magazines, photographs, and videos to the World Wide Web. As you know, a great strength of the Internet is that it includes a wide range of search and retrieval technologies that make finding information fast and easy. However, this capability also makes it easy to access, disseminate, and trade pornographic images and videos, including child pornography. As a result, child pornography has become accessible through Web sites, chat rooms, newsgroups, and the increasingly popular peer-to-peer technology, a form of networking that allows direct communication between computer users so that they can access and share each other's files (including images, video, and software).

As requested, in my remarks today, I will summarize the results of a review that we recently conducted to determine

- the ease of access to child pornography on peer-to-peer networks;
- the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography; and
- the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks.

We also include an attachment that briefly discusses how peer-to-peer file sharing works.

Results in Brief

It is easy to access and download child pornography over peer-to-peer networks. We used KaZaA, a popular peer-to-peer file-sharing program,[2] to search for image files, using 12 keywords known to be associated with child pornography on the Internet.[3] Of 1,286 items identified in our search, about 42 percent were associated with child pornography images. The remaining items included 34 percent classified as adult pornography and

[1] U.S. General Accounting Office, *File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography*, GAO-03-351 (Washington, D.C.: Feb. 20, 2003).

[2] Other popular peer-to-peer applications include Gnutella, BearShare, LimeWire, and Morpheus.

[3] The U.S. Customs CyberSmuggling Center assisted us in this work. Because child pornography cannot be accessed legally other than by law enforcement agencies, we relied on Customs to download and analyze image files. We performed analyses based on titles and file names only.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00146 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.096

24 percent as nonpornographic. In another KaZaA search, the Customs CyberSmuggling Center used three keywords to search for and download child pornography image files. This search identified 341 image files, of which about 44 percent were classified as child pornography and 29 percent as adult pornography. The remaining images were classified as child erotica[4] (13 percent) or other (nonpornographic) images (14 percent). These results are consistent with observations of the National Center for Missing and Exploited Children, which has stated that peer-to-peer technology is increasingly popular for the dissemination of child pornography. Since 2001, when the center began to track reports of child pornography on peer-to-peer networks, such reports have increased more than fourfold—from 156 in 2001 to 757 in 2002.

When searching and downloading images on peer-to-peer networks, juvenile users can be inadvertently exposed to pornography, including child pornography. In searches on innocuous keywords likely to be used by juveniles, we obtained images that included a high proportion of pornography: in our searches, the retrieved images included adult pornography (34 percent), cartoon pornography[5] (14 percent), and child pornography (1 percent); another 7 percent of the images were classified as child erotica.

We could not quantify the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks. Law enforcement agencies that work to combat child exploitation and child pornography do not track their resource use according to specific Internet technologies. However, law enforcement officials told us that as they receive more tips concerning child pornography on peer-to-peer networks, they are focusing more resources in this area.

Background

Child pornography is prohibited by federal statutes, which provide for civil and criminal penalties for its production, advertising, possession, receipt, distribution, and sale.[6] Defined by statute as the visual depiction of a minor—a person under 18 years of age—engaged in sexually explicit conduct,[7] child pornography is unprotected by the First Amendment,[8] as it is intrinsically related to the sexual abuse of children.

[4] Erotic images of children that do not depict sexually explicit conduct.

[5] Images of cartoon characters depicting sexually explicit conduct.

[6] See chapter 110 of Title 18, United States Code.

[7] *See* 18 U.S.C. § 2256(8).

[8] See *New York v. Ferber*, 458 U.S. 747 (1982).

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00147 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.097

In the Child Pornography Prevention Act of 1996,[9] Congress sought to prohibit images that are or appear to be "of a minor engaging in sexually explicit conduct" or are "advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct." In 2002, the Supreme Court struck down this legislative attempt to ban "virtual" child pornography[10] in *Ashcroft v. The Free Speech Coalition*, ruling that the expansion of the act to material that did not involve and thus harm actual children in its creation is an unconstitutional violation of free speech rights. According to government officials, this ruling may increase the difficulty of prosecuting those who produce and possess child pornography. Defendants may claim that pornographic images are of "virtual" children, thus requiring the government to establish that the children shown in these digital images are real. Recently, Congress enacted the PROTECT Act,[11] which attempts to address the constitutional issues raised in *The Free Speech Coalition* decision.[12]

The Internet Has Emerged as the Principal Tool for Exchanging Child Pornography

Historically, pornography, including child pornography, tended to be found mainly in photographs, magazines, and videos.[13] With the advent of the Internet, however, both the volume and the nature of available child pornography have changed significantly. The rapid expansion of the Internet and its technologies, the increased availability of broadband Internet services, advances in digital imaging technologies, and the availability of powerful digital graphic programs have led to a proliferation of child pornography on the Internet.

[9] Section 121, P.L. 104-208, 110 Stat. 3009-26.

[10] According to the Justice Department, rapidly advancing technology has raised the possibility of creating images of child pornography without the use of a real child ("virtual" child pornography). Totally virtual creations would be both time-intensive and, for now, prohibitively costly to produce. However, the technology has led to a ready defense (the "virtual" porn defense) against prosecution under laws that are limited to sexually explicit depictions of *actual* minors. Because the technology exists today to alter images to disguise the identity of the real child or make the image seem computer-generated, producers and distributors of child pornography may try to alter depictions of actual children in slight ways to make them appear to be "virtual" (as well as unidentifiable), thereby attempting to defeat prosecution. Making such alterations is much easier and cheaper than building an entirely computer-generated image.

[11] Public Law No. 108-21 (Apr. 30, 2003).

[12] S. Rep. No. 108-2, at 13 (2003).

[13] John Carr, *Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children*, NCH Children's Charities, Children & Technology Unit (Yokohama, 2001). (http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf)

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00148 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.098

According to experts, pornographers have traditionally exploited—and sometimes pioneered—emerging communication technologies—from the dial-in bulletin board systems of the 1970s to the World Wide Web—to access, trade, and distribute pornography, including child pornography.[14] Today, child pornography is available through virtually every Internet technology (see table 1).

Table 1: Internet Technologies Providing Access to Child Pornography

Technology	Characteristics
World Wide Web	Web sites provide on-line access to text and multimedia materials identified and accessed through the uniform resource locator (URL).
Usenet	A distributed electronic bulletin system, Usenet offers over 80,000 newsgroups, with many newsgroups dedicated to sharing of digital images.
Peer-to-peer file-sharing programs	Internet applications operating over peer-to-peer networks enable direct communication between users. Used largely for sharing of digital music, images, and video, peer-to-peer applications include BearShare, Gnutella, LimeWire, and KaZaA. KaZaA is the most popular, with over 3 million KaZaA users sharing files at any time.
E-mail	E-mail allows the transmission of messages over a network or the Internet. Users can send E-mail to a single recipient or broadcast it to multiple users. E-mail supports the delivery of attached files, including image files.
Instant messaging	Instant messaging is not a dial-up system like the telephone; it requires that both parties be on line at the same time. AOL's Instant Messenger and Microsoft's MSN Messenger and Internet Relay Chat are the major instant messaging services. Users may exchange files, including image files.
Chat and Internet Relay Chat	Chat technologies allow computer conferencing using the keyboard over the Internet between two or more people.

Source: GAO.

[14] Frederick E. Allen, "When Sex Drives Technological Innovation and Why It Has to," *American Heritage Magazine*, vol. 51, no. 5 (September 2000), p. 19. (http://www.plannedparenthood.org/education/updatearch.html)
Allen notes that pornographers have driven the development of some of the Internet technologies, including the development of systems used to verify on-line financial transactions and that of digital watermarking technology to prevent the unauthorized use of on-line images.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00149 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.099

Among the principal channels for the distribution of child pornography are commercial Web sites, Usenet newsgroups, and peer-to-peer networks.[16]

Web sites. According to recent estimates, there are about 400,000 commercial pornography Web sites worldwide,[16] with some of the sites selling pornographic images of children. The child pornography trade on the Internet is not only profitable, it has a worldwide reach: recently a child pornography ring was uncovered that included a Texas-based firm providing credit card billing and password access services for one Russian and two Indonesian child pornography Web sites. According to the U.S. Postal Inspection Service, the ring grossed as much as $1.4 million in just 1 month selling child pornography to paying customers.

Usenet. Usenet newsgroups also provide access to pornography, with several of the image-oriented newsgroups being focused on child erotica and child pornography. These newsgroups are frequently used by commercial pornographers who post "free" images to advertise adult and child pornography available for a fee from their Web sites.

Peer-to-peer networks. Although peer-to-peer file-sharing programs are largely known for the extensive sharing of copyrighted digital music,[17] they are emerging as a conduit for the sharing of pornographic images and videos, including child pornography. In a recent study by congressional staff,[18] a single search for the term "porn" using a file-sharing program yielded over 25,000 files. In another study, focused on the availability of pornographic video files on peer-to-peer sharing networks, a sample of 507 pornographic video files retrieved with a file-sharing program included about 3.7 percent child pornography videos.[19]

[16] According to Department of Justice officials, other forums and technologies are used to disseminate pornography on the Internet. These include Web portal communities such as Yahoo! Groups and MSN Groups, as well as file servers operating on Internet Relay Chat channels.

[16] Dick Thornburgh and Herbert S. Lin, editors, *Youth, Pornography, and The Internet*, National Academy Press (Washington, D.C.: 2002). (http://www.nap.edu/html/youth_internet/)

[17] According to the Yankee Group, a technology research and consulting firm, Internet users aged 14 and older downloaded 5.16 billion audio files in the United States via unlicensed file-sharing services in 2001.

[18] Minority Staff, *Children's Access to Pornography through Internet File-Sharing Programs*, Special Investigations Division, Committee on Government Reform, U.S. House of Representatives (July 27, 2001). (http://www.house.gov/reform/min/pdfs/pdf_inves/pdf_pornog_rep.pdf)

[19] Michael D. Mehta, Don Best, and Nancy Poon, "Peer-to-Peer Sharing on the Internet: An Analysis of How Gnutella Networks Are Used to Distribute Pornographic Material," *Canadian Journal of Law and Technology*, vol. 1, no. 1 (January 2002). (http://cjlt.dal.ca/vol1_no1/articles/01_01_MeBePo_gnutella.pdf)

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00150 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.100

Several Agencies Have Law Enforcement Responsibilities Regarding Child Pornography on Peer-to-Peer Networks

Table 2 shows the key national organizations and agencies that are currently involved in efforts to combat child pornography on peer-to-peer networks.

Table 2: Organizations and Agencies Involved with Peer-to-Peer Child Pornography Efforts

Agency	Unit	Focus
Nonprofit		
National Center for Missing and Exploited Children	Exploited Child Unit	Works with the Customs Service, Postal Service, and the FBI to analyze and investigate child pornography leads.
Federal entities		
Department of Justice	Federal Bureau of Investigation[a]	Proactively investigates crimes against children. Operates a national "Innocent Images Initiative" to combat Internet-related sexual exploitation of children.
	Criminal Division, Child Exploitation and Obscenity Section	Is a specialized group of attorneys who, among other things, prosecute those who possess, manufacture, or distribute child pornography. Its High Tech Investigative Unit actively conducts on-line investigations to identify distributors of obscenity and child pornography.
Department of Homeland Security	U.S. Customs Service CyberSmuggling Center[a,b]	Conducts international child pornography investigations as part of its mission to investigate international criminal activity conducted on or facilitated by the Internet.
Department of the Treasury	U.S. Secret Service[a]	Provides forensic and technical assistance in matters involving missing and sexually exploited children.

Source: GAO.

[a]Agency has staff assigned to NCMEC.

[b]At the time of our review, the Customs Service was under the Department of the Treasury. Under the Homeland Security Act of 2002, it became part of the new Department of Homeland Security on March 1, 2003.

The National Center for Missing and Exploited Children (NCMEC), a federally funded nonprofit organization, serves as a national resource center for information related to crimes against children. Its mission is to find missing children and prevent child victimization. The center's Exploited Child Unit operates the CyberTipline, which receives child pornography tips provided by the public; its CyberTipline II also receives tips from Internet service providers. The Exploited Child Unit investigates and processes tips to determine if the images in question constitute a violation of child pornography laws. The CyberTipline provides investigative leads to the Federal Bureau of Investigation (FBI), U.S. Customs, the Postal Inspection Service, and state and local law enforcement agencies. The FBI and the U.S. Customs also investigate leads from Internet service providers via the Exploited Child Unit's

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00151 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.101

CyberTipline II. The FBI, Customs Service, Postal Inspection Service, and Secret Service have staff assigned directly to NCMEC as analysts.[20]

Two organizations in the Department of Justice have responsibilities regarding child pornography: the FBI and the Justice Criminal Division's Child Exploitation and Obscenity Section (CEOS).[21]

- The FBI investigates various crimes against children, including federal child pornography crimes involving interstate or foreign commerce. It deals with violations of child pornography laws related to the production of child pornography; selling or buying children for use in child pornography; and the transportation, shipment, or distribution of child pornography by any means, including by computer.

- CEOS prosecutes child sex offenses and trafficking in women and children for sexual exploitation. Its mission includes prosecution of individuals who possess, manufacture, produce, or distribute child pornography; use the Internet to lure children to engage in prohibited sexual conduct; or traffic in women and children interstate or internationally to engage in sexually explicit conduct.

Two other organizations have responsibilities regarding child pornography: the Customs Service (now part of the Department of Homeland Security) and the Secret Service in the Department of the Treasury.

- The Customs Service targets illegal importation and trafficking in child pornography and is the country's front line of defense in combating child pornography distributed through various channels, including the Internet. Customs is involved in cases with international links, focusing on pornography that enters the United States from foreign countries. The Customs CyberSmuggling Center has the lead in the investigation of international and domestic criminal activities conducted on or facilitated by the Internet, including the sharing and distribution of child pornography on peer-to-peer networks. Customs maintains a reporting link with NCMEC, and it acts on tips received via the CyberTipline from callers reporting instances of child pornography on Web sites, Usenet newsgroups, chat rooms, or the computers of users of peer-to-peer

[20] According to the Secret Service, its staff assigned to NCMEC also includes an agent.

[21] Two additional Justice agencies are involved in combating child pornography: the U.S. Attorneys Offices and the Office of Juvenile Justice and Delinquency Prevention. The 94 U.S. Attorneys Offices can prosecute federal child exploitation-related cases; the Office of Juvenile Justice and Delinquency Prevention funds the Internet Crimes Against Children Task Force Program, which encourages multijurisdictional and multiagency responses to crimes against children involving the Internet.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00152 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.102

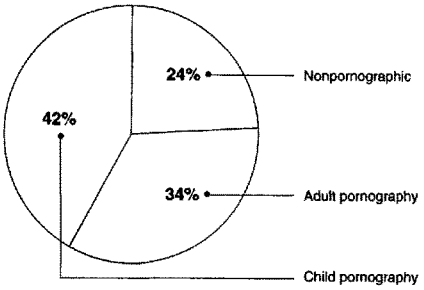
networks. The center also investigates leads from Internet service providers via the Exploited Child Unit's CyberTipline II.

- The U.S. Secret Service does not investigate child pornography cases on peer-to-peer networks; however, it does provide forensic and technical support to NCMEC, as well as to state and local agencies involved in cases of missing and exploited children.

Peer-to-Peer Applications Provide Easy Access to Child Pornography

Child pornography is easily shared and accessed through peer-to-peer file-sharing programs. Our analysis of 1,286 titles and file names identified through KaZaA searches on 12 keywords[22] showed that 543 (about 42 percent) of the images had titles and file names associated with child pornography images.[23] Of the remaining files, 34 percent were classified as adult pornography, and 24 percent as nonpornographic (see fig. 1). No files were downloaded for this analysis.

Figure 1: Classification of 1,286 Titles and File Names of Images Identified in KaZaA Search



Source: GAO.

[22] The 12 keywords were provided by the Cybersmuggling Center as examples known to be associated with child pornography on the Internet.

[23] We categorized a file as child pornography if one keyword indicating a minor and one word with a sexual connotation occurred in either the title or file name. Files with sexual connotation in title or name but without age indicators were classified as adult pornography.

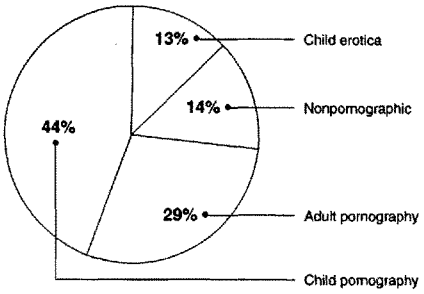
VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00153 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.103

The ease of access to child pornography files was further documented by retrieval and analysis of image files, performed on our behalf by the Customs CyberSmuggling Center. Using 3 of the 12 keywords that we used to document the availability of child pornography files, a CyberSmuggling Center analyst used KaZaA to search, identify, and download 305 files, including files containing multiple images and duplicates. The analyst was able to download 341 images from the 305 files identified through the KaZaA search.

The CyberSmuggling Center analysis of the 341 downloaded images showed that 149 (about 44 percent) of the downloaded images contained child pornography (see fig. 2). The center classified the remaining images as child erotica (13 percent), adult pornography (29 percent), or nonpornographic (14 percent).

Figure 2: Classification of 341 Images Downloaded through KaZaA



Source: Customs CyberSmuggling Center.

Note: GAO analysis of data provided by the Customs CyberSmuggling Center.

These results are consistent with the observations of NCMEC, which has stated that peer-to-peer technology is increasingly popular for the dissemination of child pornography. However, it is not the most prominent source for child pornography. As shown in table 3, since 1998, most of the child pornography referred by the public to the CyberTipline was found on Internet Web sites. Since 1998, the center has received over 76,000 reports of child pornography, of which 77 percent concerned Web sites, and only 1 percent concerned peer-to-peer networks. Web site referrals have grown from about 1,400 in 1998 to over 26,000 in 2002—or about a nineteenfold increase. NCMEC did not track peer-to-peer referrals until 2001. In 2002,

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00154 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.104

peer-to-peer referrals increased more than fourfold, from 156 to 757, reflecting the increased popularity of file-sharing programs.

Table 3: NCMEC CyberTipline Referrals to Law Enforcement Agencies, Fiscal Years 1998–2002

	Number of tips				
Technology	**1998**	**1999**	**2000**	**2001**	**2002**
Web sites	1,393	3,830	10,629	18,052	26,759
E-mail	117	165	120	1,128	6,245
Peer-to-peer	—	—	—	156	757
Usenet newsgroups & bulletin boards	531	987	731	990	993
Unknown	90	258	260	430	612
Chat rooms	155	256	176	125	234
Instant Messaging	27	47	50	80	53
File Transfer Protocol	25	26	58	64	23
Total	**2,338**	**5,569**	**12,024**	**21,025**	**35,676**

Source: Exploited Child Unit, National Center for Missing and Exploited Children.

Juvenile Users of Peer-to-Peer Applications May Be Inadvertently Exposed to Pornography

Juvenile users of peer-to-peer networks face a significant risk of inadvertent exposure to pornography when searching and downloading images. In a search using innocuous keywords likely to be used by juveniles searching peer-to-peer networks (such as names of popular singers, actors, and cartoon characters), almost half the images downloaded were classified as adult or cartoon pornography. Juvenile users may also be inadvertently exposed to child pornography through such searches, but the risk of such exposure is smaller than that of exposure to pornography in general.

To document the risk of inadvertent exposure of juvenile users to pornography, the Customs CyberSmuggling Center performed KaZaA searches using innocuous keywords likely to be used by juveniles. The center image searches used three keywords representing the names of a popular female singer, child actors, and a cartoon character. A center analyst performed the search, retrieval, and analysis of the images. These searches produced 157 files, some of which were duplicates. From these 157 files, the analyst was able to download 177 images..

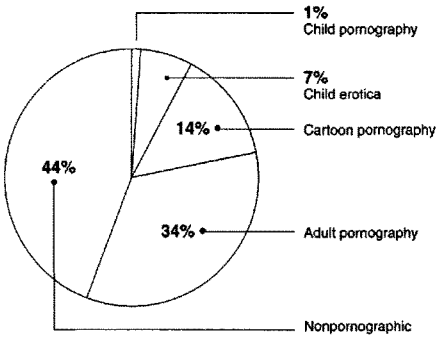
Figure 3 shows our analysis of the CyberSmuggling Center's classification of the 177 downloaded images. We determined that 61 images contained

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00155 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.105

adult pornography (34 percent), 24 images consisted of cartoon pornography (14 percent), 13 images contained child erotica (7 percent), and 2 images (1 percent) contained child pornography. The remaining 77 images were classified as nonpornographic.

Figure 3: Classification of 177 Images of a Popular Singer, Child Actors, and a Cartoon Character Downloaded through KaZaA



Source: Customs CyberSmuggling Center.

Federal Law Enforcement Agencies Are Beginning to Focus Resources on Child Pornography on Peer-to-Peer Networks

Because law enforcement agencies do not track the resources dedicated to specific technologies used to access and download child pornography on the Internet, we were unable to quantify the resources devoted to investigations concerning peer-to-peer networks. These agencies (including the FBI, CEOS, and Customs) do devote significant resources to combating child exploitation and child pornography in general. Law enforcement officials told us, however, that as tips concerning child pornography on the peer-to-peer networks increase, they are beginning to focus more law enforcement resources on this issue. Table 4 shows the levels of funding related to child pornography issues that the primary organizations reported for fiscal year 2002, as well as a description of their efforts regarding peer-to-peer networks in particular.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00156 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.106

Table 4: Resources Related to Combating Child Pornography on Peer-to-Peer Networks in 2002

Organization	Resources[a]	Efforts regarding peer-to-peer networks
National Center for Missing and Exploited Children	$12 million to act as national resource center and clearinghouse for missing and exploited children $10 million for law enforcement training $3.3 million for the Exploited Child Unit and the CyberTipline $916,000 allocated to combat child pornography	NCMEC referred 913 tips concerning peer-to-peer networks to law enforcement agencies.
Federal Bureau of Investigation	$38.2 million and 228 agents and support personnel for Innocent Images Unit	According to FBI officials, they have efforts under way to work with some of the peer-to-peer companies to solicit their cooperation in dealing with the issue of child pornography.
Justice Criminal Division, Child Exploitation and Obscenity Section	$4.38 million and 28 personnel allocated to combating child exploitation and obscenity offenses	The High Tech Investigative Unit deals with investigating any Internet medium that distributes child pornography, including peer-to-peer networks.
U.S. Customs Service CyberSmuggling Center	$15.6 million (over 144,000 hours) allocated to combating child exploitation and obscenity offenses[b]	The center is beginning to actively monitor peer-to-peer networks for child pornography, devoting one half-time investigator to this effort. As of December 16, 2002, the center had sent 21 peer-to-peer investigative leads to field offices for follow-up.

Source: GAO and agencies mentioned.

[a]Dollar amounts are approximate.

[b]Customs was unable to separate the staff hours devoted or funds obligated to combating child pornography from those dedicated to combating child exploitation in general.

An important new resource to facilitate the identification of the victims of child pornographers is the National Child Victim Identification Program, run by the CyberSmuggling Center. This resource is a consolidated information system containing seized images that is designed to allow law enforcement officials to quickly identify and combat the current abuse of children associated with the production of child pornography. The system's database is being populated with all known and unique child pornographic images obtained from national and international law enforcement sources and from CyberTipline reports filed with NCMEC. It will initially hold over 100,000 images collected by federal law enforcement agencies from various sources, including old child pornography magazines.[24] According to Customs officials, this information will help, among other things, to determine whether actual children were used to produce child pornography images by matching them with images of children from magazines published before modern imaging technology

[24] According to federal law enforcement agencies, most of the child pornography published before 1970 has been digitized and made widely available on the Internet.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00157 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.107

was invented. Such evidence can be used to counter the assertion that only virtual children appear in certain images.

The system, which became operational in January 2003,[25] is housed at the Customs CyberSmuggling Center and can be accessed remotely in "read only" format by the FBI, CEOS, the U.S. Postal Inspection Service, and NCMEC.

In summary, Mr. Chairman, our work shows that child pornography as well as adult pornography is widely available and accessible on peer-to-peer networks. Even more disturbing, we found that peer-to-peer searches using seemingly innocent terms that clearly would be of interest to children produced a high proportion of pornographic material, including child pornography. The increase in reports of child pornography on peer-to-peer networks suggests that this problem is increasing. As a result, it will be important for law enforcement agencies to follow through on their plans to devote more resources to this technology and continue their efforts to develop effective strategies for addressing this problem.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other Members of the Committee may have at this time.

Contact and Acknowledgements

If you should have any questions about this testimony, please contact me at (202) 512-6240 or by E-mail at koontzl@gao.gov. Key contributors to this testimony were Barbara S. Collier, Mirko Dolak, James M. Lager, Neelaxi V. Lakhmani, James R. Sweetman, Jr., and Jessie Thomas.

[25] One million dollars has already been spent on the system, with an additional $5 million needed for additional hardware, the expansion of the image database, and access for all involved agencies. The 10-year lifecycle cost of the system is estimated to be $23 million.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00158 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.108

Attachment: How File Sharing Works on Peer-to-Peer Networks

Peer-to-peer file-sharing programs represent a major change in the way Internet users find and exchange information. Under the traditional Internet client/server model, access to information and services is accomplished by interaction between *clients*—users who request services—and *servers*—providers of services, usually Web sites or portals. Unlike this traditional model, the peer-to-peer model enables consenting users—or *peers*—to directly interact and share information with each other, without the intervention of a server. A common characteristic of peer-to-peer programs is that they build virtual networks with their own mechanisms for routing message traffic.[26]

The ability of peer-to-peer networks to provide services and connect users directly has resulted in a large number[27] of powerful applications built around this model.[28] These range from the SETI@home network (where users share the computing power of their computers to search for extraterrestrial life) to the popular KaZaA file-sharing program (used to share music and other files).

As shown in figure 4,[29] there are two main models of peer-to-peer networks: (1) the centralized model, in which a central server or broker directs traffic between individual registered users, and (2) the decentralized model, based on the Gnutella[30] network, in which individuals find each other and interact directly.

[26] Matei Ripenau, Ian Foster, and Adriana Iamnitchi, "Mapping the Gnutella Network: Properties of Large Scale Peer-to-Peer Systems and Implication for System Design," *IEEE Internet Computing*, vol. 6, no. 1 (January–February 2002). (people.cs.uchicago.edu/~matei/PAPERS/ic.pdf)

[27] Zeropaid.com, a file-sharing portal, lists 88 different peer-to-peer file-sharing programs available for download. (http://www.zeropaid.com/php/filesharing.php)

[28] Geoffrey Fox and Shrideep Pallickara, "Peer-to-Peer Interactions in Web Brokering Systems," *Ubiquity*, vol. 3, no. 15 (May 28–June 3, 2002) (published by Association of Computer Machinery). (http://www.acm.org/ubiquity/views/g_fox_2.html)

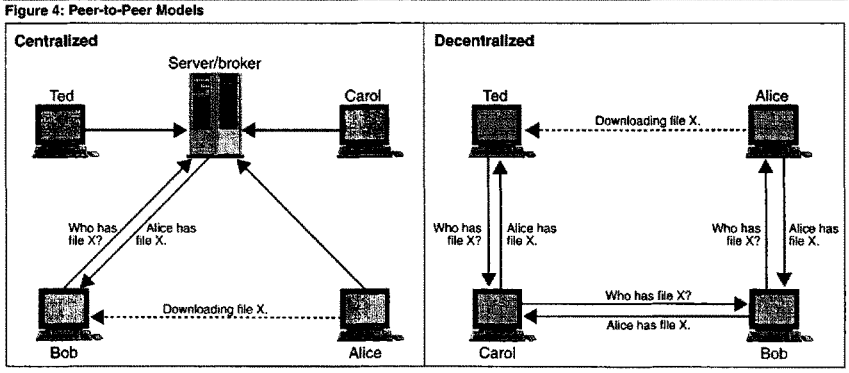
[29] Illustration adapted by Lt. Col. Mark Bontrager from original by Bob Knighten, "Peer-to-Peer Computing," briefing to Peer-to-Peer Working Groups (August 24, 2000), in Mark D. Bontrager, *Peering into the Future: Peer-to-Peer Technology as a Model for Distributed Joint Battlespace Intelligence Dissemination and Operational Tasking*, Thesis, School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, Alabama (June 2001).

[30] According to LimeWire LLC, the developer of a popular file-sharing program, Gnutella was originally designed by Nullsoft, a subsidiary of America Online. The development of the Gnutella protocol was halted by AOL management shortly after the protocol was made available to the public. Using downloads, programmers reverse-engineered the software and created their own Gnutella software packages. (http://www.limewire.com/index.jsp/p2p)

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00159 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.109

Figure 4: Peer-to-Peer Models



Source: Mark Bontreger, Bob Knighten.

As shown in figure 4, in the centralized model, a central server/broker maintains directories of shared files stored on the computers of registered users. When Bob submits a request for a particular file, the server/broker creates a list of files matching the search request by checking it against its database of files belonging to users currently connected to the network. The broker then displays that list to Bob, who can then select the desired file from the list and open a direct link with Alice's computer, which currently has the file. The download of the actual file takes place directly from Alice to Bob.

This broker model was used by Napster, the original peer-to-peer network, facilitating mass sharing of material by combining the file names held by thousands of users into a searchable directory that enabled users to connect with each other and download MP3 encoded music files. Because much of this material was copyrighted, Napster as the broker of these exchanges was vulnerable to legal challenges,[31] which eventually led to its demise in September 2002.

In contrast to Napster, most current-generation peer-to-peer networks are decentralized. Because they do not depend on the server/broker that was the central feature of the Napster service, these networks are less vulnerable to litigation from copyright owners, as pointed out by Gartner.[32]

In the decentralized model, no brokers keep track of users and their files. To share files using the decentralized model, Ted starts with a networked computer equipped with a Gnutella file-sharing program such KaZaA or

[31] *A&M Records v. Napster*, 114 F.Supp.2d 896 (N.D. Cal. 2000).

[32] Lydia Leong, "RIAA vs.Verizon, Implications for ISPs," Gartner (Oct. 24, 2002).

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00160 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.110

BearShare. Ted connects to Carol, Carol to Bob, Bob to Alice, and so on. Once Ted's computer has announced that it is "alive" to the various members of the peer network, it can search the contents of the shared directories of the peer network members. The search request is sent to all members of the network, starting with Carol; members will in turn send the request to the computers to which they are connected, and so forth. If one of the computers in the peer network (say, for example, Alice's) has a file that matches the request, it transmits the file information (name, size, type, etc.) back through all the computers in the pathway towards Ted, where a list of files matching the search request appears on Ted's computer through the file-sharing program. Ted can then open a connection with Alice and download the file directly from Alice's computer.[33]

The file-sharing networks that result from the use of peer-to-peer technology are both extensive and complex. Figure 5 shows a map or topology of a Gnutella network whose connections were mapped by a network visualization tool.[34] The map, created in December 2000, shows 1,026 nodes (computers connected to more than one computer) and 3,752 edges (computers on the edge of the network connected to a single computer). This map is a snapshot showing a network in existence at a given moment; these networks change constantly as users join and depart them.

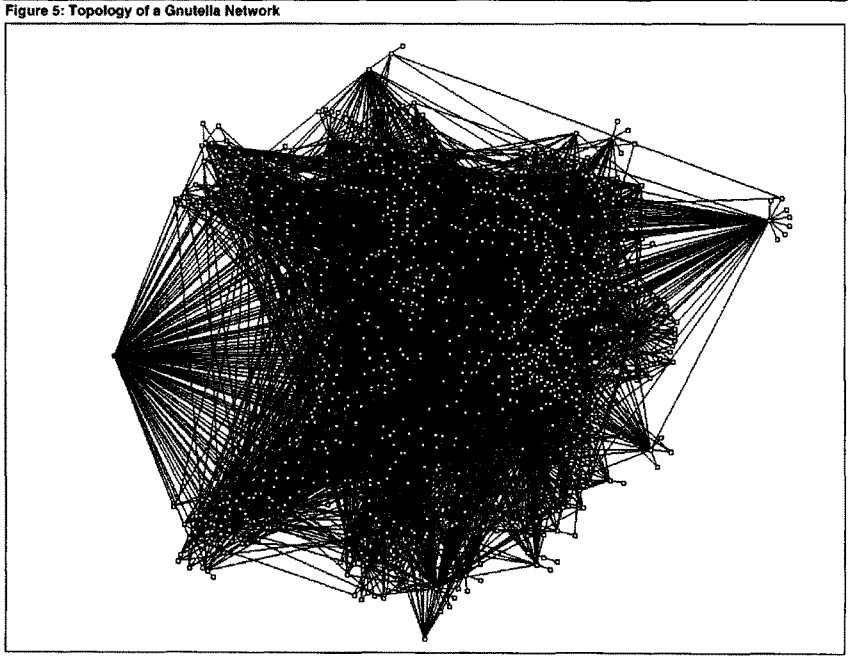
[33] LimeWire, *Modern Peer-to-Peer File Sharing over the Internet.* (http://www.limewire.com/index.jsp/p2p)

[34] Mihajlo A. Jovanovic, Fred S. Annexstein, and Kenneth A. Berman, *Scalability Issues in Large Peer-to-Peer Networks: A Case Study of Gnutella*, University of Cincinnati Technical Report (2001). (http://www.ececs.uc.edu/~mjovanov/Research/paper.html)

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00161 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.111

Figure 5: Topology of a Gnutella Network



Source: Mihajlo A. Jovanovic, Fred S. Annexstein, and Kenneth A. Berman, Laboratory of Networks and Applied Graph Theory, University of Cincinnati.

One of the key features of many peer-to-peer technologies is their use of a virtual name space (VNS). A VNS dynamically associates user-created names with the Internet address of whatever Internet-connected computer users happen to be using when they log on.[36] The VNS facilitates point-to-point interaction between individuals, because it removes the need for users and their computers to know the addresses and locations of other users; the VNS can, to certain extent, preserve users' anonymity and provide information on whether a user is or is not connected to the Internet at a given moment. Peer-to-peer users thus may appear to be

[36] S. Hayward and R. Batchelder, "Peer-to-Peer: Something Old, Something New," Gartner (Apr. 10, 2001).

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00162 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.112

anonymous; they are not, however. Law enforcement agents may identify users' Internet addresses during the file-sharing process and obtain, under a court order, their identities from their Internet service providers.

(310381)

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00163 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.113

U.S. SENATOR PATRICK LEAHY

CONTACT: David Carle, 202-224-3693 VERMONT

Statement of Senator Patrick Leahy
Senate Committee on the Judiciary
Hearing on "Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks"
September 9, 2003

At the first Committee hearing on peer-to-peer networks in June, we considered the significant dangers that file sharing can pose to users' privacy and to the security of their computers. Today, we will begin to explore possible solutions to some of the problems raised by peer-to-peer networks and online file sharing. Unless some solutions are found, peer-to-peer will never realize its enormous potential to build on-line communities, to enhance networked learning, and to make unprecedented amounts of material, educational and entertaining, available worldwide.

I believe that peer-to-peer has the potential to revolutionize the way people share all sorts of information. But as with any technology, it can be abused. Peer-to-peer networks can be used to delve into people's private records, or illegally to share copyrighted material. Most disturbingly, peer-to-peer networks can be used to distribute child pornography, and to make all sorts of pornography available to unsuspecting children. If peer-to-peer networks are going to find a useful place in our culture, they must respond to these problems. And we certainly cannot allow those who purposefully exploit network file-sharing to the detriment of children to go unpunished.

As a father and grandfather, I find child pornography despicable. I know my colleagues agree with me. This Committee and the Senate as a whole have taken strong steps to protect our children from pornography, and we will continue to do everything possible to combat child pornography. As a former prosecutor, I want to see that law enforcement has effective tools for the identification and prosecution of the individuals who make, use, and traffic in this material.

Pornography, and child pornography in particular, is prevalent on peer-to-peer networks. According to recent reports, as much as 42 percent of peer-to-peer requests are for pornography. A recent GAO study was a wake-up call for America. It found that simple keyword searches on a peer-to-peer network turned up hundreds of pornographic images of children. In fact, child pornography constituted 40 percent of the returns to those searches. The National Center for Missing and Exploited Children, which

senator_leahy@leahy.senate.gov
http://leahy.senate.gov/

93014.114

continues to do outstanding and inspirational work to protect all of our children, reports that there has been a fourfold increase in pornography on peer-to-peer networks in just

one year. Moreover, peer-to-peer networks don't simply allow the distribution of child pornography. Through the use of instant messaging, they can be used to lure children into meeting with sexual predators.

So far the peer-to-peer networks are not only turning a blind eye to this problem; in many cases they are specifically designed so that parents are unable to keep their children off the network with a traditional firewall. In addition, what few protections are available are designed so that they can be easily circumvented by a child, regardless of their parent's intentions.

More disturbingly, the networks are actively hindering law enforcement efforts to crack down on child pornography. Although pornography on peer-to-peer has risen fourfold between 2001 and 2002, arrests for child pornography have dropped dramatically in recent years. We have heard that one, and perhaps the only, reason for this is that peer-to-peer networks have changed their systems to allow their users to remain anonymous. In their zeal to allow illegal file sharing, the networks have made it far too difficult for law enforcement to track down child pornographers. This must stop.

I look forward to hearing from the outstanding group of experts that we have assembled here today about what steps can be taken to stop child pornography. This problem is best solved by the people who understand it best, and deal with it on a daily basis. I am eager to work with those involved as they craft a private-sector solution to this very serious problem, but make no mistake: This must stop.

The second panel today will look at one of the solutions to online file sharing that we enacted five years ago as part of the Digital Millennium Copyright Act. The DMCA gave law enforcement and copyright holders powerful new tools to use in the fight against online copyright infringement.

At the time we were drafting the DMCA, the recording industry, the internet service providers, and others said they were having trouble identifying individuals who might be illegally sharing copyrighted materials online. The parties came together and determined that the best solution was to allow copyright holders to subpoena the information. The subpoena would go to the internet service provider, and would seek the identity of someone the individual believed to be sharing copyrighted material on that ISP's system or network. Section 512(h) of the DMCA codified this solution.

I understand that this section is now being used to subpoena information about individual users who may be sharing copyrighted material, but who are not using the ISP's system or network to store the copyrighted material. In short, it is being used to combat the anonymous use of peer-to-peer networks. There can be little doubt that the use of the 512(h) subpoena raises legitimate concerns for some, such as notice to the end user, oversight of the subpoena process, and the cost of responding to the subpoenas. As

93014.115

before, I believe that these problems are best solved by the groups most closely involved. I look forward to hearing what collaborative steps are being taken to address these concerns, and to make the 512(h) subpoena the fair, but strong tool we intended it to be.

# # # # #

Statement of John Malcolm
Deputy Assistant Attorney General
Criminal Division

Before the Committee on the Judiciary
United States Senate

Regarding Peer-to-Peer Networks and Child Pornography

September 9, 2003

Mr. Chairman, Senator Leahy, and distinguished Members of the Committee, thank you for inviting me to testify before you today on this critical topic. The sexual abuse of a child is a horrific act, and this horror is often exacerbated by pedophiles who memorialize their repugnant crimes in photographs and videos. Sadly, with increasing frequency, such offenders are choosing to disseminate these grotesque memorials to millions of people over the Internet with a few clicks of a computer mouse.

The exploitation of children through the production and dissemination of child pornography is an intolerable evil that we must work to obliterate. Toward that end, Congress recently made significant strides by enacting the PROTECT Act, which provides invaluable tools to law enforcement to aggressively prosecute crimes involving the scourge of child pornography. Nevertheless, child pornographers continue to find ways to employ the ever-evolving technology of the Internet and computers to commit their deviant crimes. In turn, law enforcement must respond to technological advances, as well, eradicating child pornographers from every forum in which they lurk, be that in cyberspace or otherwise. Thus, I commend you for holding this hearing. I hope to provide you with an understanding of how peer-to-peer file-sharing computer networks are being used to distribute and receive child pornography, how pornography in general is being made available to children over peer-to-peer networks, and how the Department of

93014.117

Justice is attempting to root out those who are taking advantage of technology to distribute child pornography.

At the outset, it is important to acknowledge the Department's firm belief in the positive aspects of the Internet. In too many instances, people view government officials, especially those who work in federal law enforcement, as anti-technology — intent only on stifling the growth of technology and the Internet. This is simply not the case. The Internet's benefits are too numerous and obvious to restate here, and the Department of Justice supports the full development of the Internet and technology. But, just as law enforcement must operate in a way that does not unnecessarily impede the advancement of technology, so too must people acknowledge that technology is often misused to perpetrate criminal activity which can, in and of itself, undermine public confidence in those technologies and impede their advancement.

Before I address the Department of Justice's approach to the proliferation of child pornography over peer-to-peer file-sharing networks, let me first describe how these so-called "P2P" networks operate. From this common understanding of the technology, we can see how P2P networks are being abused by child pornographers, the unique issues that arise in regard to criminal prosecutions involving P2P networks, and how the use of P2P networks to disseminate child pornography fits into the greater context of child pornography crimes being committed on the Internet.

BACKGROUND ON PEER-TO-PEER FILE-SHARING NETWORKS

First let me contrast peer-to-peer networks with the more traditional network that is used to share computer files. On traditional networks, people who want to share files — including

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00168 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.118

contraband files — store them on one or more central "servers," which are powerful computers that supply the files to a number of smaller, less powerful computers such as the computer you might have at your desk. Picture a bicycle wheel, where the server computer is the hub that sends files out through the spokes to smaller computers arrayed along the tire. A file that is available on one customer's desktop is not available to any other computer on the network until it is uploaded to the central server.

The peer-to-peer network, by contrast, is less centralized; in fact, it is fluid by design. If a traditional network looks like a bicycle wheel, a peer-to-peer network looks like a fisherman's net. Each peer computer is connected to the rest of the peer computers either directly or through one or more intermediary computers. In a P2P network, files are kept not on a central server but, rather, on each of the peer computers hooked into the network at any given point in time.

Any peer computer, which could be the computer sitting on your child's desktop, can be utilized to download P2P software from the Internet and thereby gain access to shared files located on other computers connected to that network. Once the software is installed, P2P networks can be accessed to transfer virtually anything that can be put into digital format, including pictures, music, or videos. A user may search the P2P network for files based on certain characteristics such as a keyword or file name, for example, and may narrow his or her search to identify only video files, images or audio files. The P2P software then displays a list of shared files matching the search criteria that are currently available from other computers connected to the network. Once the user selects those files that he wishes to download, the source and destination peer computers exchange files directly. Similarly, a user may also elect to share certain files on his own computer with other users on the P2P network. Given this format,

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00169 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.119

it is not surprising that this medium has become a hotbed of criminal activity, particularly where child pornography is concerned.

POTENTIAL FOR CRIMINAL ACTIVITY THROUGH USE OF PEER-TO-PEER FILE-SHARING NETWORKS

The potential for criminal activity through the use of peer-to-peer networks is no secret to the members of this Committee. The possibilities include privacy and security intrusions; copyright infringement; the dissemination of adult pornography to children; and, as underscored by this hearing, the distribution of child pornography.

Privacy and Security Intrusions

Peer-to-peer file-sharing software is associated with three types of potential privacy or security intrusions. The first potential intrusion comes when a user installs the peer-to-peer software on his computer. Some P2P software is intentionally infected by adware, spyware, and even viruses or so-called "Trojan horses," which are applications that appear benign but contain latent viruses. Thus, merely installing P2P software can expose a peer computer to attack. The next type of intrusion may occur when the user tells the P2P software what files to share. P2P users have inadvertently given other people access to their tax returns, medical files, financial records, personal e-mail, and confidential legal documents such as attorney-client communications. The final type of intrusion may occur once the user starts sharing files with others. Hackers have exploited the openness of P2P networks to propagate viruses, worms, and other malicious computer software. Sadly, but predictably, at least one virus propagated itself over a peer-to-peer network in part by renaming itself as computer files that promised

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00170 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.120

pornographic images. This combination of vulnerabilities makes using a peer-to-peer file-sharing network a very risky proposition indeed.

Copyright Infringement

At this point there should be no doubt that even if P2P networks can be used for legitimate purposes, a large number of people are using P2P networks for copyright infringement. Given how P2P networks operate, it is easy to see why. P2P networks involve millions of users, and because they are increasingly fast, users can download files with relatively little risk of detection. The Department of Justice will fight copyright infringement in any medium in which it takes place, and I have therefore specifically directed the Department's Computer Crime and Intellectual Property Section to consider means for combating copyright infringement over P2P networks.

Distribution of Adult Pornography that is Legal, But Easily Seen by Children

Congress is well aware that adult pornography is readily available to children on the World Wide Web and is often inadvertently accessed by children using innocuous search terms, such as the names of cartoon characters or children's television shows. Indeed, to combat this growing problem, Congress, through the PROTECT Act, recently enacted a law criminalizing the use of domain names that mislead minors into viewing harmful material.

Despite the potency of this new legislation, it does not extend to file names that individuals create for files on their computers that they choose to share over P2P networks. Thus, any child who downloads P2P software and enters an innocuous search term may be confronted with files containing adult pornography that have been given misleading names. On a

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00171 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.121

positive note, most P2P software packages contain filters that can be activated to screen out adult material and/or digital images, and many of these filters are password protected, so that children cannot deactivate filters that their parents have activated.

Distribution of Child Pornography

Like all other Internet venues, P2P networks are fertile ground for the distribution and receipt of child pornography. The design of P2P networks allows perpetrators readily to identify numerous desired files on other users' computers using fairly blatant search terms, such as "child porn" or "lolita." Users can then download materials relatively quickly for their personal possession and use and retreat into obscurity.

LAW ENFORCEMENT ISSUES UNIQUE TO PEER-TO-PEER NETWORKS

Because peer-to-peer networks operate as a diffuse community of computers, the investigation of child pornography offenses in the peer-to-peer context requires a proactive and focused approach by law enforcement. The lack of a central server means that there is no clearinghouse for files and information that can serve as a bottleneck or choke point where law enforcement can gather logged evidence of illegal activity and cut off the supply of contraband files. Moreover, the decentralized nature of P2P networks means that there is no central community where people communicate regarding their illegal plans. Instead, peer-to-peer file-sharing networks are diffuse in nature: millions of people can join loosely-knit groups without the need for humans to communicate at all, since their computers will automatically handle all of the details for them. The only entrance fee to an illegal group is the time to download P2P software, boot it up, and start uploading and downloading files.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00172 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.122

Relative Anonymity

As compared with Internet access in general or email accounts, many P2P networks do not require individual users to set up an account with a central authority. P2P users can create and change user names at will, and user names rarely contain any information that would reveal the true identity of the user.

Nevertheless, just as an individual cannot receive or place a telephone call without a telephone number, every instance of Internet access is associated with in internet protocol, or "IP," address. Thus, using P2P software, a law enforcement agent can identify a file containing child pornography, and while downloading that file, identify the IP address of the computer sending it. The agent can then determine which Internet service provider owns that IP address, and serve legal process on that Internet service provider to obtain the name and address of the P2P user associated with that IP address on the date and time that the file was shared. Moreover, seizure of that user's computer will often reveal the IP addresses of other computers with which contraband files were shared. Thus, although it is true that absent an undercover operation, there is relatively little risk of detection on P2P networks, no P2P user is truly "anonymous."

Notably, however, new generations of P2P file-sharing protocols and tools are promising their users even more anonymity, such as by hiding IP addresses behind proxy servers or even refusing to recognize preliminary inquiries from computers known to be associated with law enforcement. Some peer-to-peer tools are even touting their ability to shield users from the view of victims or law enforcement. Should this technology come to fruition, it will present significant challenges to law enforcement and will undoubtedly make P2P an even more popular

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00173 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.123

vehicle for trading child pornography.

THE DEPARTMENT OF JUSTICE'S EFFORTS CONCERNING THE DISTRIBUTION OF CHILD PORNOGRAPHY OVER PEER-TO-PEER NETWORKS

The Department of Justice is committed to vigorously prosecuting child pornography in every forum in which it appears, including the myriad channels of access available on the Internet. Certainly, P2P networks are of significant law enforcement concern and focus, particularly because of their decentralized design and relative accessibility and ease of use. The Department has established a High Tech Investigative Unit within the Child Exploitation and Obscenity Section dedicated to providing investigative support in prosecutions for crimes involving child exploitation and obscenity, and specifically, child pornography on the Internet, including in P2P networks. Consistent with the Department's mission to eradicate child pornography, the Federal Bureau of Investigation is currently considering a protocol for investigating child pornography cases in the relatively new area of P2P technology.

While there is no question that there is a plethora of pornographic and obscene material on P2P networks, which is easily accessible by children, it is difficult to quantify what percentage of the dissemination of child pornography on the Internet occurs via P2P networks. The General Accounting Office ("GAO") report released on March 13, 2003 indicates that, while reports on P2Ps have increased, ultimately only 1 percent of the tips from the public received by the National Center for Missing and Exploited Children since 1998 involved P2P technology.

There are several other avenues of Internet communication that, for a number of reasons, currently hold significant appeal for purveyors and seekers of child pornography. Among the most popular of these are commercial web sites, newsgroups, and internet relay chats, or "IRCs."

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00174 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.124

Arguably the most troublesome of these are commercial web sites. Even greater than the percentage of the computer-literate population that has ever utilized P2P software is the percentage of people who have utilized web sites; indeed, nearly everyone old enough to type words on a computer keyboard understands how to "surf the web" and access websites on topics of interest. Computers are sold with Internet browser software pre-installed. Capitalizing on the accessibility and commensurate popularity of the Web, child pornographers offer images and video files for sale on a vast number of commercial websites hosted on servers throughout the world. These websites often boast "extreme" and varied material, for which child pornographers typically have a seemingly insatiable desire. The increasing demand drives the market for child pornography on the Web. As a result, the financial profits associated with the exploitation of children through such sites can be staggering. Undercover purchases and the utilization of legal process to obtain credit card and billing records can lead to extensive investigations and prosecutions in these types of cases.

Slightly more savvy computer users utilize IRCs to obtain child pornography. Through IRCs, individuals communicate in real time with other users currently online. Such users can advertise the files that they possess on their computers, and invite others to download those files for a price. A typical user will set up "rules" for access to his file collection. Thus, for example, a user will allow another user to download 5 images only if that person first uploads 3 images. A user may further specify that he only wants pictures of "girls under 10" or "father-son incest." Many times, the user sets his computer to scan uploaded images to ensure that the images he is receiving are not duplicative of those already in his collection. The user may also threaten to ban individuals from future trading if they do not abide by his rules, for example, by uploading

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00175 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.125

inauthentic images. Sometimes, users offer a "free look" at small files to entice others to trade.

Once a user identifies a desirable potential source of new files, the donor and recipient go into a "private" window and their computers communicate directly to facilitate the downloading and uploading of images. Using IRCs, a child pornographer can increase the size and diversity of his collection, which collectors of child pornography characteristically and compulsively seek to do. By contrast, offering files on P2P does not automatically result in receiving files in return, making it a less appealing prospect. IRC users can be targeted through undercover operations, just as P2P users can, with one added benefit: because IRCs operate through centralized servers, the service providers frequently retain records of communications, albeit for short periods of time, which can be obtained through legal process.

Perhaps the most popular aspect of Internet use is communication via email; only marginally more technical than email are newsgroups. By joining newsgroups dedicated to a given subject matter, users can communicate by email with like-minded individuals regarding their common interests. Thus, there are newsgroups dedicated to football, cooking, astronomy, and - - not surprisingly - - child pornography. Newsgroups are attractive to child pornographers because, like IRCs, they precipitate trading relationships. Law enforcement can target newsgroups through undercover trading and subsequent use of subpoenas or court orders for the records of internet service providers.

CONCLUSION

It is my hope that I have provided the Committee with a clearer understanding of peer-to-peer technology, its implications for the dissemination of child pornography, and where it fits

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00176 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.126

into the larger context of the proliferation of child pornography on the Internet. Most assuredly, the Department of Justice is committed to eradicating child pornography in every possible venue through an aggressive prosecution strategy.

Mr. Chairman, I again thank you and the Committee for the opportunity to speak to you today, and I would be pleased to answer any questions the Committee might have.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00177 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.127

Statement of Mr. Alan Morris, Executive Vice President,

Sharman Networks Limited

Before the

Senate Judiciary Committee

Regarding

"Pornography, Technology and Process: Problems and Solutions on Peer-to-Peer Networks"

Washington, DC

September 9, 2003

Chairman Hatch and members of the Committee, thank you for this opportunity to again share the views of Sharman Networks Limited (SNL) regarding peer-to-peer (P2P) technology. I am Sharman's Executive Vice President and, as it is a global business, I am responsible for supervising the enterprise from London whilst our Sydney headquarters is off-line at night. I also have specific responsibility for developing the promotion and distribution of licensed content in conjunction with Altnet, our Los Angeles-based U.S. business partner. The Altnet service is available to all users of the Kazaa Media Desktop (KMD) software. Altnet is the largest distributor in the world of licensed and protected media files, as well as the leading purveyor of files utilizing Microsoft Windows Media digital rights management (DRM) technology.

Since its creation, SNL has been dedicated to two principal goals. The first goal is to fully exploit the potential for P2P software to enrich society and the creators of intellectual property through the development of this most efficient means for the commercial distribution of copyrighted material. The second is to provide consumers with the most secure and best functioning P2P software available anywhere; we are the industry leader and consumers have validated our efforts by making the Kazaa Media Desktop (KMD) the most popular P2P application. So, we have built the technology platform for achieving our premier goal, and will be announcing a series of exciting new ventures with content providers throughout the world in coming months. Our greatest disappointment in this regard is that major U.S. content providers have yet to acknowledge that P2P is not the problem but the solution to their digital dilemma and license their copyrighted material for paid distribution to KMD users.

P2P Misinformation

Unfortunately, certain Hollywood interests have not just failed to acknowledge the positive role that P2P can play in solving their online distribution challenge, but have embarked on a deliberate campaign to try to smear P2P

93014.128

technology itself. It seems that ever since Federal District Judge Stephen Wilson's April ruling that the distribution of P2P software was a legal activity in the United States under the standard established by the Supreme Court's 1984 "Betamax" decision, entertainment industry lobbyists have accelerated their deliberate campaign of P2P misinformation on Capitol Hill.

When I testified before you in June I took many of those charges head on and, I believe, showed you that the concerns raised were spurious. You learned that KMD includes, at no cost, highly effective anti-virus protection; last month this feature validated P2P as the distribution technology of the future in response to the MSBlast scare by distributing a massive 10 Terabytes of antivirus update files seamlessly over P2P in a single week, with none of the load problems encountered at this time of peak demand by traditional anti-virus distribution. We also apprised you of SNL's firm "no spyware" policy. And we described the extensive changes we had made to the KMD user interface and installation process to eliminate any possibility of identity theft as a result of inadvertent placement of personal information in a user's shared folder, even though the FBI had apprised Congress that it did not know of a single instance of I.D. theft resulting from the use of P2P software. Our testimony also quoted various experts' Congressional testimony that P2P software did not have intrinsic security weaknesses or present different or greater security problems than such common Internet tools as web browsers or e-mail software.

Since we presented that testimony, intervening events have further substantiated our position. Two major electronic virus infestations caused several $billion in damage to computer systems over the summer, and in both cases the principal means of propagation was the exploitation of known weaknesses in commonly used server and e-mail software, with P2P playing no role – indeed, as I noted, it was a major force in combating it. And, just last week, the Federal Trade Commission released its Identity Theft Survey Report; in recounting the means by which I.D. thieves gain access to the personal information of their victims, P2P does not even get a mention. As the saying goes, while P2P's detractors are entitled to their own opinions, they are not entitled to their own facts.

Zero Tolerance for Child Pornography

Mr. Chairman, there is one allegation being made against P2P software that we find vile and reprehensible. And that is the charge that there is some strong linkage between the use of such software and the propagation of exploitive and illegal child pornography. Let me make Sharman Network's position on such despicable content crystal clear. We utterly abhor child pornography. We do not want our software used to propagate this filth, even if it is in a small way.

93014.129

Since acquiring the KMD software early in 2002 we have had only a handful of case requests about specific child pornography available through P2P from law enforcement agencies worldwide. In each case we proved willing to immediately work with officers. However, they realized very quickly what their colleagues elsewhere had determined some while before –

- Pedophiles quickly realized, when P2P first appeared, that it was a foolhardy way to pursue their warped ends. To make their "collections" publicly available on P2P is counter to their cloak of secrecy. Law enforcement agencies quickly picked them off and so they retreated back to their sordid encrypted sites, newsgroups and the like.
- The nature of p2p applications, unlike websites with their central servers, means that software developers like SNL have about as much knowledge and control over what individuals choose to share as Microsoft has over what is sent via its e-mail clients!
- The relatively small amount of child pornography circulating on P2P has been hypothesized as being largely the legacy of these early forays rather than the stream of new material that pervades the chosen means of pedophile distribution.

Not satisfied just to see this small amount of material wither away (see chart at end of statement) we are actively working with U.S. and international law enforcement authorities, including the FBI, to provide them with a technical understanding of the software and, whilst clarifying the limitations in knowing systemically about files transacted, we have pointed out how they may use readily available technologies to help identify specific users who share illegal pornographic material. Law enforcement agencies, of course, may obtain through appropriate legal process the willing cooperation of ISPs and others in the chain of transmission the necessary proof to pursue and arrest miscreants. In this regard we applaud the actions of Suffolk County police authorities in arresting individuals who have used KMD or other P2P applications to share illegal content and hope other police agencies follow suit. We want pedophiles to quickly get the message that when they make such materials available for other P2P users to find they are also making it quite easy for law enforcement authorities to find them, and then cease to use P2P as a means of propagating child pornography.

In short, Sharman Networks has a zero tolerance policy in regard to child pornography, and we stand ready to take whatever additional feasible steps a software distributor can take to assist in reducing this problem still further. It should be noted that, while we support user privacy, SNL has not chosen to use methods of providing anonymity to users that could hinder the legitimate quests for purveyors of obscene material by law enforcement agencies.

So, we ask that you put P2P's role in perspective as regards the very real and growing problem of child pornography on the Internet. Based upon the data we have seen, such as that contained in the General Accounting Office's

93014.130

February report on this subject (GAO-03-351) and the chart reproduced below, P2P plays a very minor role in the propagation of child pornography. P2P referrals presently constitute less than two percent of all reports of child pornography submitted to the CyberTipline operated by the National Center for Missing and Exploited Children, while Internet Web sites account for more than seventy seven percent. While any amount of child pornography available via P2P software is unacceptable to us, we know of no instance or charge that there is any commercial or organized distribution of such materials using P2P, while many of the thousands of Web sites hosting child pornography do charge for access to these illegal materials, and newsgroups are actively used for illegal private distribution.

Commercial child pornography Web sites are a rapidly growing problem. Last month, the United Kingdom's National Criminal Intelligence Service released a report stating that Websites containing child pornography had more than doubled in the past year, that more than half of them were hosted in the United States, and that Internet pedophiles were developing more cunning means of avoiding detection. Clearly, any effective law enforcement initiative against the child pornography problem must be primarily directed against these Web sites and coordinated on an international basis

Mr. Chairman, it is clear that the vast majority of the child pornography problem stems from Web sites accessed by Web browser software. Yet we do not see a coordinated campaign to smear Web browsing technology even though it is the primary technological means by which child pornography is accessed, distributed, and sold. Nor do we see such a campaign against instant messaging software, chat rooms or news groups, even though there have been repeated reports of how pedophiles have masqueraded as minors and used these technologies to engage in suggestive conversations with minors, to send pornographic images to minors, and to attempt to set up face to face meetings with minors. And we certainly do not see misguided legislative initiatives, such as a bill recently introduced in the House of Representatives that aims to ban the distribution of P2P technology, directed at these other major technological tools which are commonly subverted by pedophiles for their evil purpose. Nor should we, because we all know that technologies are not inherently good or evil – what's good or bad are the uses that individuals put them to; and what should be pursued are those bad actors that use them for evil ends.

It seems the reason that the entertainment industry has tried to create an unwarranted association between child pornography and P2P is not because P2P software plays a major role in this illicit trade but because they want to create sufficient animosity against this technology to assist in the enactment of new legislation that weakens Betamax standard protection, requires copy control technology, regulates P2P out of existence, or otherwise supports Hollywood's goal of subjugating technology to the needs of their existing business models. This ploy was admitted by unnamed record industry executives in a September

93014.131

2nd Los Angeles Times article: *"Even as the RIAA prepares to seize parents' attention with lawsuits, music executives increasingly have been trying to call attention to the fact that file swapping networks also are frequently used to share child pornography and other X-rated images. Record executives say privately they're also aiming to use the proliferation of pornography as a means of persuading members of Congress and law enforcement officials to take a tougher stance against the file networks."*

This may be seen as hypocritical, to say the least, from an industry which quickly wraps itself in your First Amendment whenever the content it produces and the advertising that promotes it are criticized for graphic and gratuitous sex and violence and the promotion of substance abuse. The difference is that the entertainment industry actively markets such fare to kids -- Sharman just provides technology that can be used or misused.

Barring Minors' Access to Legal Adult Content

Most adult content is legal, and its availability in our society is a fact of life, with major corporations engaged in its distribution. It's sold on nearly every newsstand. It's marketed on both a subscription and pay-per-view basis to customers of satellite and cable TV and guests at major hotel chains. The ability to watch X-rated movies in the privacy of one's own home was a driving force in the adoption of the VCR, and this content has migrated onto DVDs as that new technology supplants video tape. And it's well known that access to adult content and sex-oriented chat rooms was an important factor in the growth of now major ISPs, and that the sale of legal adult content is one of the major Internet commerce success stories as well as being touted as the "killer content" for new generation 3G phones.

So it should come as no surprise that one use that individuals make of P2P software is to access adult content. SNL does not distribute any such content. Altnet does have a paid publishing system that allows content owners to publish content into the system. A legal review is always conducted on all such content before publishing takes place. Following the high standards of satellite TV and the cable industry, Altnet does not discriminate against publishers that work within the law and provide technical restrictions to prevent unauthorized distribution of content that may be unsuitable to children. Any adult content published via Altnet is of course only available, through strict credit card verification, to persons over eighteen years of age.

Other individual software users provide the great majority of the adult content available to users of the KMD software. SNL has no direct knowledge of what any particular user is providing, nor do we have any ability to control such distribution or remove a particular piece of content. What we can do, and in fact do, is to provide KMD users, at no charge, with the most comprehensive and

93014.132

effective, password protected, family filter available with any P2P software application.

The extensive availability of offensive materials on popular search engines, such as Yahoo and Google, is a concern for everyone. For instance, a search for the most commonly used adult term on Google will return 43,600.000 results! This does not mean Google is inherently bad. To the contrary, it simply reflects the vast amount of pornography accessible from websites that minors may access in the absence of parental oversight, in contrast to the relatively small amount available from peers' shared folders via P2P.

Like these companies, we are making great efforts to educate users and to aggressively encourage the use of our built in family filter. This filter is set to "on" as the default when the KMD software is first downloaded. Upon acquiring KMD in 2002 we thought it particularly important that such a filter be made an integral part of the software and be turned on as default. This has been validated by the finding of the June 2003 report, "Fast and Present Danger: In-Home Study on Broadband Security Among American Consumers", a study conducted by America Online for the National Cyber Security Alliance, that in 97% of homes with broadband connections parents failed to employ any parental controls to block access to the vast array of adult materials available on tens of thousands of Internet Web sites. Our family filter also provides parents with a password-protected lock so that it cannot be turned off when they are out of the house. We believe it should always be used in households where children may have access to the PC. We also believe filters can never take the place of active and involved parenting.

The KMD filter is based on a confidential list of keywords (unsurprisingly culled from the terms used on the major search engines) associated with adult content and other offensive materials. No adult content filter, no matter how it works, can ever be 100 percent effective at blocking such content. That is particularly true when individuals deliberately create false metatags so that offensive content may be found in a search for innocent material. Similarly some files are salaciously or misleadingly labeled, however innocent or obscene the content might be. There is nothing unique to P2P in this regard. Just last week, the U.S. attorney for the Southern District of New York, in conjunction with the U.S. Postal Inspection Service, made the first arrest under the Truth in Domains Names Act. They charged an individual with creating at least 3,000 misleading domain names, such as dinseyland.com, so that individuals making common typing mistakes, including children, would be connected to advertising sites, including those for pornographic materials, from which they could not easily exit. Announcing the arrest, U.S. Attorney James Comey stated, "The defendant is accused of taking advantage of children's common mistakes, and using that to profit by leading them by the hand into the seediest and most repugnant corners of cyberspace. His alleged actions are not clever but criminal."

93014.133

We abhor such practices and we welcome any suggestions as to how we might increase the protections against unwanted exposure to adult materials available through the use of P2P technology. But, whether children are using Web browsers, instant messaging software, chat rooms or P2P software, the best means of preventing unwanted exposure to offensive materials is for parents to employ available safeguards such as KMD's family filter, and to actively monitor their children's Internet activities while periodically reviewing both the software and content on their home computer hard drives.

Conclusion

We appreciate this opportunity to share our views regarding pornography and P2P software. We are dedicated to the eradication of child pornography from P2P networks and will continue to cooperate with Congress, law enforcement agencies, and dedicated nongovernmental agencies in support of that shared goal. We are constantly updating the terms blocked by the KMD family filter and will take all other feasible steps to best assure that minors are not inadvertently exposed to adult content when using the KMD software. We have also helped to found a new trade group, the Distributed Computing Industry Association (DCIA), which is designed to bring together all business interests with a stake in P2P technology to collectively address shared challenges, including pornography.

We hope that this Committee and the Congress as a whole will, as they address this issue, keep in mind the many responsible actions that Sharman Networks has taken in regard to adult content, as well as the relatively minor role that P2P plays in the overall availability of such content on the Internet.

I would be pleased to answer your questions.

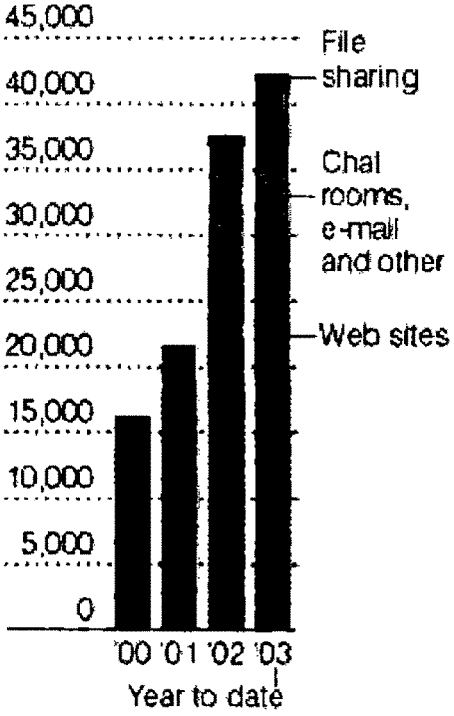
93014.134

Source: New York Times, September 7, 2003

Where Danger Lurks Online

Some complaints about child pornography on the Internet focus on file-sharing networks like KaZaA, but over all file sharing makes up a small and shrinking portion of all reported child pornography.

Reported child pornography sightings



Source: National Center for Missing and Exploited Children

93014.135

Committee on the Judiciary
United States Senate
September 9, 2003
Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks
Statement of the Honorable Marybeth Peters,
Register of Copyrights

Mr. Chairman, Senator Leahy, Members of the Committee, good afternoon. It is always a pleasure to appear before this Committee and I thank you for inviting me to present the views of the Copyright Office today at this very timely hearing. As you were among the leaders in drafting and enacting the Digital Millennium Copyright Act ("DMCA"), I know that these issues are important to you, as they are to me.

I. Background

In 1999, a young man named Shawn Fanning developed a use of the Internet that allowed people to identify and copy music files from other people's computers. As you know, this model popularized peer-to-peer technology and a company called Napster tried to turn it into a profit-making business. Napster became phenomenally popular in a remarkably short period of time, boasting millions of registered users the very next year. But it quickly became clear that Napster was being used extensively (by millions of users) for the purpose of copying and distributing an unprecedented number of copyrighted works, primarily sound recordings of musical works.

That was the scene when you held a hearing on July 11, 2000, Mr. Chairman, entitled "Music on the Internet: Is There an Upside to Downloading?" At that hearing, Mr. Hank Barry, then the CEO of Napster, stated "It is my firm belief that the consumers who use Napster are *not* committing copyright violations."[1] We did not agree with that assessment,[2] and we were

---

[1] Submitted Testimony, Hank Barry, p. 7(emphasis in original).

[2] See Brief for the United States as *Amicus Curiae* at 11, n.1, 18, *A&M Records, Inc. v. Napster*, 293 F.3d 1004 (9th Cir. 2001)(Nos. 00-16401 & 00-16403).

93014.136

heartened when the Ninth Circuit found that "Napster users infringe at least two of the copyright holders' exclusive rights: the rights of reproduction...and distribution."[3] Napster was unable to find a way to continue operations and faded away.

The void left by Napster's departure was filled by other businesses utilizing peer-to-peer technology, such as Aimster, Grokster, and Kazaa. While some of these applications can be differentiated from Napster in terms of their internal technical operation, they still follow the same basic peer-to-peer model as Napster and it is apparent that an overwhelming number of their customers are using it for the same purpose as they and others had used Napster – copying and distributing copyrighted works. By now it is well-settled that those users are infringing copyright. Notwithstanding that, there are still some who contend that such uses are not infringing.[4]

Mr. Chairman, make no mistake. The law is unambiguous. Using peer-to-peer networks to copy or distribute copyrighted works without permission is infringement and copyright owners have every right to invoke the power of the courts to combat such activity. Every court that has addressed the issue has agreed that this activity is infringement.[5] It can also be a crime and the perpetrators of such a crime are subject to fines and jail time.

Some have tried to rationalize or justify their illegal behavior by attacking the victim with allegations of inflated profits or unfair dealings with recording artists on the part of the recording

---

[3] *A&M Records v. Napster*, 293 F.3d 1004, 1014 (9th Cir. 2001)(hereinafter "*Napster*").

[4] Los Angeles Times, 'Tone Deaf to a Moral Dilemma?" (Sept. 2, 2003).

[5] See *Napster* at 1014; *In re: Aimster Copyright Litigation*, 334 F.3d 643, 645 (7th Cir. 2003)(hereinafter "*Aimster*"); *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F.Supp. 2d 1029, 1034-35 (C.D. Cal. 2003)(hereinafter "*Kazaa*").

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00187 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.137

industry. These diversionary tactics do not alter the fundamental fact that they are trying to defend illegal activity that takes place on peer-to-peer networks. For those who do not have sympathy for the recording industry, there are other victims as well. Since Napster, subsequent versions of peer-to-peer networks permit infringement of the works of other copyright owners, large and small, from motion picture studios to independent photographers and needlepoint designers. With broadband connections becoming more and more widespread, it is increasingly more common that the larger files containing full-length motion pictures are copied back and forth.[6] This problem is not shrinking; it is not static; it is growing.

There are some who argue that copyright infringement on peer-to-peer systems is not truly harmful to copyright owners and may even help them generate new interest in their products. The law leaves that judgment to the copyright owner and it ought not be usurped by self-interested third parties who desire to use the copyright owner's work.

II. Copyright Liability of Peer-to-Peer Proprietors

Copyright law has long recognized that those who aid and abet copyright infringement are no less culpable than the direct infringers themselves.[7] There are two types of this secondary liability. Contributory infringement occurs when "[o]ne who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another."[8] For purposes of this test, knowledge can be either actual or constructive – that is, having reason to

---

[6] See Gary Gentile, "Online Movie Service Quickens Downloads," Associated Press, September 3, 2003.

[7] See *Kalem Co. v. Harper Bros.*, 222 U.S. 55, 63 (1911).

[8] *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00188 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.138

know.[9] Vicarious liability occurs when one "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[10]

Both of these concepts were brought to bear in the case against Napster. The Ninth Circuit agreed with the District Court that Napster had actual knowledge of the infringements it was facilitating from, for example, notices from aggrieved copyright owners.[11] There was little question but that Napster provided a material contribution in the form of "the site and facilities" for infringement.[12] Thus, Napster was determined to be a contributory infringer.

The Ninth Circuit also considered whether Napster was vicariously liable. It had no difficulty agreeing with the District Court that the infringing material on its network was a "draw" for customers, thus providing a direct financial benefit from the infringing activity.[13] The Ninth Circuit also agreed with the District Court that Napster had the ability to police its system, and thus that it had the right and ability to supervise its users' conduct.[14] Accordingly, Napster was found to be vicariously liable as well.

Thus it was that many felt reassured that the Ninth Circuit had confirmed that copyright law provides an effective and efficient way in which to address the massive infringements that

---

[9] *Id.*

[10] *Id.*

[11] *Napster* at 1020-21.

[12] *Id. at 1022 (quoting Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996)(hereinafter *"Fonovisa"*)).

[13] *Id.* at 1023 (quoting *Fonovisa* at 263-64).

[14] *Id.* at 1023-24.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00189 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.139

can and do occur on peer-to-peer networks. Unfortunately, the *Napster* decision was not the final word on the matter.

Earlier this year, the Central District of California surprised many when it held that Grokster and Kazaa are not liable as secondary copyright infringers.[15] This decision departed from long-established precedent. For example, the court held that in order to establish contributory liability, it must be shown that "a defendant has actual – not merely constructive – knowledge of the infringement at a time during which the defendant materially contributes to that infringement."[16] Were such a standard to be adopted it would eviscerate the doctrine of contributory infringement as it would be almost impossible to meet. It would encourage the kind of sophistry we have seen from the proprietors of some peer-to-peer applications: a denial of knowledge of infringements by their customers in the face of clear and uncontested evidence that such infringement is occurring on a mind-boggling scale. Mr. Chairman, these are people whose business plan is dependant upon massive copyright infringement and any application of the law that allows them to escape liability for lack of knowledge of those same infringements is inherently flawed.

Not only was the *Kazaa* decision wrong on the law, it has serious policy consequences as well. The historical doctrines of secondary liability have served copyright owners, courts, and the public well – they provide copyright owners with the ability to obtain relief against the root cause of a series of infringements without costly, inefficient, and burdensome suits against

---

[15] *Kazaa*, 259 F.Supp. 2d 1029.

[16] *Id.* at 1036.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00190 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.140

numerous individuals.[17] Without a viable doctrine of contributory liability, this option is severely curtailed and may present the copyright owner with the unenviable choice of either accepting unremedied infringements or filing numerous suits against the individual direct infringers.

If today's hearing leaves the Committee with the impression that the law is in flux with regard to the liability of proprietors of peer-to-peer technology, that is because it is. On one side is the *Napster* decision of the Ninth Circuit and the *Aimster* decision of the Seventh Circuit, both finding liability, albeit through different paths of analysis. On the other side is the *Kazaa* decision of the Central District of California, finding no liability for Kazaa and Grokster. Hanging over all of these cases is the Supreme Court's decision in *Sony*. It is perhaps a commentary on that opinion that almost twenty years later, we still have such uncertainty that three courts seem to interpret and apply it in three different ways. I believe that the correct application of the doctrines of secondary liability and the *Sony* case should produce findings of liability for the proprietors of Kazaa and Grokster as well as Napster and Aimster. If the case law evolves so as to compel the opposite result, I believe that *Sony* should be revisited either by the Supreme Court or by Congress.

III. Suits Against Individuals

Unless and until the *Kazaa* decision is overruled, copyright owners are faced with the unenviable choice to which I referred earlier. They can either resign themselves to unremedied infringements on a previously unimaginable scale, or they can file infringement actions against individual peer-to-peer users. The recording industry has chosen the latter route.

---

[17] See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 437, n. 18(hereinafter "*Sony*")(citing the "dance hall cases"); *Fonovisa*, 76 F.3d 259 (suit against the operator of a swap meet for infringing activity of third-party vendors).

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00191 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.141

While copyright owners have expressed regret that they have felt compelled to take this step, they need offer no apologies. As I have already said, people who use peer-to-peer technology for the unauthorized reproduction or distribution of copyrighted works are breaking the law. Surprisingly, many people do not appear to realize this. I have long advocated more public education about copyright. In a perfect world, this could be done in classrooms and with billboards. But ours is not a perfect world, and public education can also be accomplished through enforcement of copyright.

The threats of litigation and even the publicity about the subpoenas obtained by the RIAA have made clear to everyone that the so-called "file-sharing" of copyrighted works is not an innocent activity without legal consequences. As a result, it is becoming more and more difficult for people engaged in such activity to claim that they did not know what they were doing is against the law. Of course, for some users of peer-to-peer technology, even knowledge that what they are doing is illegal will not be a sufficient disincentive to engage in such conduct. But whether or not these infringers know or care that it is against the law, the knowledge that such conduct may lead to expensive and burdensome litigation and a potentially large judgment should have a healthy deterrent effect. While we would like to think that everyone obeys the law simply because it is the law and out of a sense of obligation, we also know that laws without penalties may be widely ignored. For many people, the best form of education about copyright in the internet world is the threat of litigation. In short, if you break the law, you should be prepared to accept the consequences. Copyright owners have every right to enforce their rights in court, whether they are taking action against providers of peer-to-peer services designed to profit from copyright infringement or against the persons engaging in individual acts of infringement

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00192 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.142

using such services.

IV. Statutory History and Interpretation of Subsection 512(h)

It is common sense that in order to be able to take action against the users of peer-to-peer networks, the copyright owner must know who those users are.[18] Congress foresaw this need and addressed it by including in the DMCA a process by which copyright owners can learn basic identifying information about alleged infringers from their internet service providers ("ISPs").[19]

The DMCA began as an effort to implement the 1996 WIPO Internet treaties.[20] Neither those treaties nor any other international instrument directly address the potential secondary liability of ISPs. However, as the treaty implementing legislation moved forward in Congress, representatives of ISPs demanded that the legislation also limit their liability under such circumstances.[21] Congress heeded this call and provided the ISPs with a huge benefit - virtually no liability for qualifying ISPs. This was balanced by a carefully developed set of obligations in the DMCA. Among those balancing obligations was the requirement that ISPs "expeditiously" respond to subpoenas to provide identifying information about subscribers accused of copyright infringement so that the controversy could be settled in court.

At the time the DMCA was drafted, at least one representative of ISPs assured this

---

[18] The existence of section 512(h) is plain evidence that Congress did not view any existing procedures by which a suit could be filed against an unknown defendant as acceptable alternatives for copyright owners.

[19] See 17 U.S.C. §512(h).

[20] See *Hearings on S. 1121 Before the Senate Judiciary Committee*, 105th Cong. 25 (statement of George Vradenburg, III)(representing "over 1,400 Internet service providers, content creators, telephone companies, among others...).

[21] *Id.*

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00193 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.143

Committee that ISPs desired a solution whereby "service providers and content owners...work as a partnership...."[22] It was asserted by that same representative that "[l]iability for copyright infringement should fall where it belongs, on the Web site operators, on those who create an infringing work or on those who reproduce it or perform it with actual knowledge of the infringement...."[23] The ability of copyright owners to utilize subsection 512(h) is a critical part of that partnership as is copyright owners' ability to impose liability against those who infringe copyright. It is regrettable that at least one major ISP now rejects the compromise and the balance of the DMCA.

Some now claim that the subpoena power of subsection 512(h) is inapplicable to the activity described in subsection 512(a). As the United States District Court for the District of Columbia recently held, the plain language of subsection 512(h) demonstrates that this interpretation is not correct.[24] I agree with the court's analysis.

Subsection 512(h) instructs service providers to expeditiously respond to a subpoena. The definition of "service provider" in section 512(k) always includes service providers which qualify for the safe harbor in section 512(a). The court reasoned that this demonstrates Congress' intent to apply the subpoena power to "all service providers, regardless of the functions a service provider may perform under the four categories set out in subsections (a) through (d)."[25]

---

[22] *Id.*

[23] *Id.*

[24] *In re: Verizon Internet Services, Inc., Subpoena Enforcement Matter*, 240 F.Supp. 2d 24, 30 (D.D.C. 2003).

[25] *Id.* at 31.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00194 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.144

It has also been argued that the subpoena power applies only to subsection 512(c) because subsection 512(h)(2)(A) requires a copyright owner to supply "a copy of a notification described in subsection (c)(3)(A)". However, as the District Court pointed out, subsection 512(h) "is written without limitation or restriction as to its application."[26] It does not require that a notice be delivered. Had Congress wished to limit the application of the subpoena power, it would have simply said so in the law. It did not.[27]

The statutory text confirms the policy of compromise behind subsection 512 -- that copyright owners and ISPs work together to remedy infringement. Limiting the subsection 512(h) subpoena provisions as some have proposed would remove an important tool that parties need to remedy infringement efficiently in the peer-to-peer context.

When it enacted the DMCA, Congress did not carve out an exception from subsection 512(h) for transitory digital network communications, the activity covered by subsection 512(a). Service providers which engage in that activity received the benefits and burdens of the same bargain that service providers engaged in the other activity covered by section 512 received. In exchange for a powerful limitation on liability, they undertook some obligations, including the obligation to identify alleged infringers when served with a subsection 512(h) subpoena. When you enacted section 512, you made the right choice. There is no reason for the courts or Congress to have second thoughts about that decision.

I understand that the majority if not all of the 512(h) subpoenas that have been sought, have been sought in the United States District Court for the District of Columbia. Apparently

---

[26] *Id.* at 33.

[27] *Id.*

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00195 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.145

this has necessitated the clerk of that court assigning additional staff to handle the workload. I do not take a position as to whether it is appropriate for a copyright owner to go to a single district court for subpoenas to service providers located outside that district. However, I am sympathetic to concerns about efficiency of the courts and fairness to ISPs located elsewhere in the country. There would certainly be advantages to the filing of these subpoena requests in the districts in which the ISPs are located.

V. Constitutional Challenges to Subsection 512(h)

The United States has intervened in the Verizon-RIAA litigation to defend the constitutionality of the DMCA. The Copyright Office has assisted the Justice Department in this effort and we firmly believe that subsection 512(h) is appropriate and constitutional. Although I am not an expert on constitutional law and I am not here to represent the Department of Justice, I will briefly summarize the arguments the United States made in its brief to the District Court.

The claim that subsection 512(h) violates the case and controversy requirement of the Constitution is belied by a review of other federal laws providing similar procedures, at least one of which has a 150 year pedigree.[28] The 512(h) procedure is also similar to discovery in advance of federal litigation pursuant to Federal Rule of Procedure 27, which finds its origins in the Judiciary Act of 1789.[29] Further, the subpoena power provided in subsection 512(h) does relate to cognizable Article III controversies, namely potential copyright infringement action as well as

---

[28] Brief for Intervenor United States of America, p. 6, *In re: Verizon Internet Services, Inc., Subpoena Enforcement Matter*, 257 F.Supp. 2d 244 (D.D.C. 2003)(No. 03-MS-0040 (JDB)).

[29] *Id.* at 10-11.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00196 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.146

a dispute between the copyright owner and the ISP over access to the subscriber information.[30]

The claim that subsection 512(h) violates the First Amendment does not withstand scrutiny. Subsection 512(h) does not proscribe spoken words or expressive or communicative conduct,[31] nor is there a realistic danger that it will significantly compromise a recognized First Amendment protection.[32] Section 512(h) merely requires a service provider to identify a person who appears to be engaging in copyright infringement, a necessary step before the copyright owner can initiate legal action. That action may range from an email or letter demanding that the alleged infringer cease and desist from the unlawful conduct to the filing of a lawsuit for copyright infringement. Section 512(h) does not offend the First Amendment any more than the filing of a lawsuit for copyright infringement. In fact, it is an essential tool for a copyright owner who intends to file such a lawsuit. Moreover, indeed, section 512 imposes sanctions on those who misuse the subpoena power, which serve to provide a safeguard.[33]

Although not addressed in the Government's briefs in intervention, I think it is important to put into context the privacy claims that some now put forward. Users of peer-to-peer networks are, by definition, opening their computers up to the world. There may be an illusion of anonymity to that activity, but we have come to learn that such connections can also make available the user's social security number, credit card numbers, and other vital information. By contrast, the 512(h) subpoena process typically involves disclosure to the copyright owner of no

---

[30] *Id.* at 9, 13.

[31] *Id.* at 15-16.

[32] *Id.* at 16-18.

[33] *Id.* at 17-18.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00197 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.147

more than the subscriber's name, email address, phone number, and perhaps street address. This hardly seems like an invasion of privacy.

VI. Conclusion

The DMCA represents a carefully crafted and balanced bargain which utilizes the incentives created by pre-existing doctrines such as secondary liability as well as enlightened self-interest to encourage all stakeholders to work cooperatively to realize the potential of the Internet while respecting legal rights. Some are now selectively challenging key components of that bargain, particularly in the context of peer-to-peer technology. Taken together, the positions of Kazaa and Grokster, along with the arguments now made by Verizon, if they prevail, will leave copyright owners with little or no remedy against the most widespread phenomena of infringement in the history of this country. We know from past experience with Napster and current experience with Kazaa and Grokster that without a judicial remedy, this infringement will not stop, regardless of the availability of lawful alternatives. It is thus incumbent upon this Committee and this Congress to see to it that if the judiciary fails to enforce the DMCA and therefore fails to provide the protection to which copyrighted works are entitled, the legislature does.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00198 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.148

News from
Congressman Joe Pitts
Sixteenth Congressional District of Pennsylvania
204 Cannon House Office Building, Washington, DC 20515 www.house.gov/pitts (202) 225-2411 Derek Karofmar, Press Secretary

For Immediate Release
July 24, 2003

Rep. Pitts introduces bill to protect children from peer-to-peer porn

Washington—Congressman Joe Pitts (R, PA-16) today introduced the Protecting Children from Peer-to-Peer Pornography (P4) Act. The P4 Act gives parents the tools they need to protect their children from pornography and threats to privacy posed by peer-to-peer file trading networks.

"Millions of people are using peer-to-peer software at any given time. About forty percent of them are children," said Rep. Pitts. **"Unfortunately, pedophiles and pornographers use these networks to distribute pornography. If a child using this software wants to download a file, he or she can type in an innocent key word and inadvertently download pornography."**

In March 2003, the General Accounting Office (GAO) and the House Committee on Government Reform found that: pornography is readily available and accessible on P2P networks; children are easily exposed to pornography while using P2P programs; and the filters available to parents do sufficiently address the threat to their children's' safety.

"Our legislation gives parents the tools they need to protect their children from pornography and threats to privacy posed by peer-to-peer file trading networks. By working together to protect children, we are building a broad and bipartisan coalition," concluded Rep. Pitts.

The P4 Act regulates P2P software, and requires the Federal Trade Commission ("FTC") to adopt regulations that require P2P distributors to:

- Give notice of the threats posed by P2P software;
- Distribute P2P software to a minor only with a parent's consent, and not when parents have used a "do not install" beacon to indicate their desire to avoid P2P software;
- Comply with the Children's Online Privacy Protection Act (COPPA) when collecting information from children under age 13;
- Ensure that the software can be readily uninstalled; and
- Ensure that the user's computer not be commandeered as a "super node," and not disable or circumvent security or protective software, without consent.

###

93014.149

News from
Congressman Joe Pitts
Sixteenth Congressional District of Pennsylvania
204 Cannon House Office Building, Washington, DC 20515 www.house.gov/pitts (202) 225-2411 Derek Kerchner, Press Secretary

For Immediate Release
July 31, 2003

Rep. Pitts: Peer-to-peer porn indictment proof that Congress needs to act

Washington—Congressman Joe Pitts (R, PA-16) today said the indictment of twelve people for possession of child pornography obtained with peer-to-peer file trading software is evidence that Congress needs to act to protect children. Last week, Rep. Pitts introduced H.R. 2885, the Protecting Children from Peer-to-Peer Pornography Act.

"These indictments are proof that Congress needs to act to protect children from peer-to-peer software. These people got child porn using peer-to-peer software. That means children can see it and download it. And sexual predators can use it to prey on our kids," said Rep. Pitts.

The *Associated Press* reported yesterday that "a five-month joint investigation by police and investigators from the Suffolk County district attorney's office led to indictments against 11 men and one woman on felony charges of possessing child pornography or promoting child pornography." The downloaded pornographic files were obtained using peer-to-peer file trading software and included still photographs and video of children involved in sex acts. Some of the files involved babies still in diapers.

"The types of stuff these people were trading often ends up on a kid's computer screen. And parents have no way to stop it. Parents need to know what's out on these networks. And they need the means to protect their kids from people who use child porn to prey on children," concluded Rep. Pitts.

H.R. 2885 regulates P2P software, and requires the Federal Trade Commission ("FTC") to adopt regulations that require P2P distributors to:

- Give notice of the threats posed by P2P software;
- Distribute P2P software to a minor only with a parent's consent, and not when parents have used a "do not install" beacon to indicate their desire to avoid P2P software;
- Comply with the Children's Online Privacy Protection Act (COPPA) when collecting information from children under age 13;
- Ensure that the software can be readily uninstalled; and
- Ensure that the user's computer not be commandeered as a "super node," and not disable or circumvent security or protective software, without consent.

###

93014.150

New York's Senator

CHARLES E. SCHUMER

313 Hart Senate Office Building • Washington, DC 20510
Phone: (202) 224-7433 • Fax: (202) 228-1218

FOR IMMEDIATE RELEASE
September 9, 2003

CONTACT: Phil Singer
(202) 224- 7433

SCHUMER URGES CREATION OF FEDERAL TASK FORCE TO CRACK DOWN ON CHILD PORN FILE-SHARING

Many parents are unaware about how popular file-sharing software enables children to download pornography; Senate Judiciary Committee to hold hearings on Tue afternoon

Schumer, law enforcement officials and child advocacy group I-Safe will call for special task force to investigate swapping of child porn files on programs like Kazaa

Child-safety advocates and law enforcement officials joined US Senator Charles E. Schumer today in calling for the creation of a new federal task force to crack down on child pornography being swapped over popular file-sharing networks like Kazaa, Morpheus, Grokster, and Bear Share. Because these increasingly popular file-sharing networks are so easy to use, they are very attractive to child pornographers and have enabled obscene materials to sail across cyber-space at an alarming rate.

"The darkside of the Internet just keeps getting darker and darker," Schumer said. "File-sharing software programs have polluted the web for long enough, spreading child pornography at an almost unprecedented rate. The Justice Department needs to do something about this scourge before the gains we have made in cracking down on child pornogrpahy in recent years are undone."

A recent report by the General Accounting Office found that file-sharing software is an effective tool for someone trying to get their hands on child pornography. During a random search using keywords associated with pornography, the report found that 42 percent of the hits it got back contained suggestions of child pornography. The study also concluded that it would be easy for a minor to inadvertently download pornography. For example, the GAO searched for keywords commonly entered by children (like Britney Spears) and found that about half of the hits it got back could be considered pornographic.

Yesterday, the recording industry announced that it was suing 261 people who use file-sharing software to swap music over the Internet. The industry used the basic search engine on the different sharing networks that let anyone accessing the websites know what files the other users are making available. Schumer said if the recording industry has the means to track down music swappers, the Justice Department should have the ability to track down child pornographers using the file-sharing software.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00201 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.151

Schumer said a federal task force on child pornography file-sharing would complement steps that local law enforcement officials are beginning to prosecute child pornographers using file-sharing software to spread their materials. Earlier this summer, the District Attorney from Suffolk County, NY - Thomas Spota - filed criminal charges against 12 people for child pornography-related offenses as a result of sharing and downloading graphic images of children being raped and abused using the Kazaa network. The material was shared over the Internet using the same kind of software that lets people share music files with one another.

In a letter being sent to Attorney General John Ashcroft today, Schumer urged the Justice Department to establish a national task force to combat the growing child pornography epidemic on file-sharing networks.

"An important step in fighting the child pornographers who use this technology is the creation of a federal task force. A federal task force would bring together the resources and expertise of the Federal Bureau of Investigation and other federal law enforcement agencies to find the best ways to track down and stop these criminals from peddling child pornography. In addition, information sharing between the federal task force and local officials, including District Attorney Tom Spota of Suffolk County, New York, who has successfully filed charges, will ensure that all levels of law enforcement are up to speed in this highly technical area," Schumer wrote.

#####

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00202 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.152

HARLES E. SCHUMER
NEW YORK

COMMITTEES:
BANKING
JUDICIARY
RULES

United States Senate
WASHINGTON, DC 20510

September 9, 2003

The Honorable John Ashcroft
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear General Ashcroft,

I write today to urge you to establish a national task force to combat the increasingly prevalent problem of child pornography being shared over file-sharing networks. These file-sharing networks are incredibly popular; one such network, Kazaa, claims that its program has been downloaded over 270 million times. Although this software is well known as a tool for sharing music and video files, it can also be readily used to engage in other criminal behavior.

Earlier this summer, the District Attorney in Suffolk County, New York, filed criminal charges against 12 people for child pornography-related offenses as a result of sharing and downloading graphic images and video of children being abused in the most horrifying manner. This case demonstrates that effective law enforcement must keep pace with the new technology tools employed by criminals.

An important step in fighting the child pornographers who use this technology is the creation of a federal task force. A federal task force would bring together the resources and expertise of the Federal Bureau of Investigation and other federal law enforcement agencies to find the best ways to track down and stop these criminals from peddling child pornography. In addition, information sharing between the federal task force and local officials, including District Attorney Tom Spota of Suffolk County, New York, who has successfully filed charges, will ensure that all levels of law enforcement are up to speed in this highly technical area.

Peer-to-peer networks are easy to use, readily accessible and decentralized making them attractive to child pornographers. A federal task force will investigate the ways these networks are used and abused and provide the most innovative law enforcement solutions to protect our nation's children. I look forward to working with you on this important issue.

Sincerely,

Charles E. Schumer
United States Senator

93014.153

STATEMENT OF CARY SHERMAN
PRESIDENT AND GENERAL COUNSEL
RECORDING INDUSTRY ASSOCIATION OF AMERICA
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
ON
"PORNOGRAPHY, TECHNOLOGY, AND PROCESS: PROBLEMS AND SOLUTIONS ON PEER-TO-PEER NETWORKS"

SEPTEMBER 9, 2003

Introduction:

Let me begin by thanking Chairman Hatch and the Ranking Member, Senator Leahy for inviting me to testify today and for their ongoing commitment to protecting intellectual property.

My name is Cary Sherman. I am the President of the Recording Industry Association of America, the trade association representing the U.S. recording industry. RIAA members create, manufacture and/or distribute 90 percent of all legitimate sound recordings in the United States.

I'd like to take a minute to give the Committee some information regarding our announcement yesterday that we filed lawsuits against individuals who were sharing hundreds or thousands of copyrighted music files on public peer-to-peer ("P2P") networks. I'd be happy to answer any of the Committee's questions regarding our enforcement efforts.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00204 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.154

Turning my attention to the subject of today's hearing, I would like to give the Committee a sense of the gravity of the piracy problem affecting our industry because I think it helps put in context the broader issues being addressed today.

The Piracy Problem Facing the Music Industry:

To date, over the past three years shipments of recorded music in the U.S. have fallen by an astounding 31%. And worldwide, the music industry has shrunk from a $40 billion industry in 1999 down to a $26 billion industry in 2002. Hit records have been impacted most dramatically. In 2000, the ten top-selling albums in the United States sold a total of 60 million units. In 2001, that number dropped to 40 million. Last year, it totaled just 34 million.

The root cause for this drastic decline in record sales is the astronomical rate of music piracy on the Internet. According to a November 2002 survey by Peter D. Hart Research, by a 2-to-1 margin, most consumers who say they are illegally downloading more music report that they're purchasing less. The same survey found that the main reason consumers aren't buying more music is that they get a lot of what they want for free by illegally downloading or copying it from others. These findings are bolstered by a June 2003 Edison Media Research report which found that "among the heaviest downloaders, 48% say they no longer have to buy

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00205 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.155

CDs because they could download the same music for free over the Internet" – an increase of 61% in just one year. These findings are consistent with the skyrocketing number of users of peer-to-peer ("P2P") file sharing software.

As of July 2002, KaZaa -- the most popular peer-to-peer ("P2P") file-sharing network by far -- boasted 100 million registered users. By May 2003, KaZaa had become the world's most downloaded software program of any kind, with 230.3 million downloads. All told, millions of users download over 2.6 billion copyrighted files (mostly sound recordings) each month via various peer-to-peer networks.

Of course, these networks are not limited to stolen copyrighted works. A GAO Report released earlier this year reveals that a significant percentage of the files available to these 13 million new users per month are pornography, including child pornography. And the problems are not just limited to the type of files available on these systems. Recent hearings in the House Government Reform and Oversight Committee and the Senate Judiciary Committee have also highlighted the serious privacy and security threats posed by P2P software, including the fact that many users on these systems are exposing their personal documents (e.g., tax returns, resumes, and medical records) to millions of other users.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00206 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.156

Although there is no easy solution to these problems, one thing is clear: Verizon is reaping enormous financial benefits from the explosion in the use of P2P. It is particularly troubling to our industry that Verizon actively encourages its new subscribers to visit unauthorized P2P services -- instead of legitimate, licensed sites -- as their preferred source for music online.

Even as we speak, when new customers sign-up for Verizon DSL they receive a brochure entitled "Your Guide to Broadband Living & Content". Amazingly, on page 12 of the brochure, in the section that discusses music, Verizon tells its new subscribers, and I quote:

- "Once you're ready to groove to some tunes . . . [k]eep a couple of things in mind. Subscription sites do offer up MP3s to download; however, they typically don't offer music that is selling exceedingly well in stores. **By contrast, the free sites are likely to have pretty much everything, but you may get pelted with some unwanted ads.**"[1]

And people wonder why the copyright community is skeptical of Verizon's claim that the real issue is privacy and not their tacit acceptance and promotion of piracy by their subscribers.

[1] If Verizon cared as much about the privacy of their customers as they contend, one would expect them to include a prominent warning to their subscribers about the serious and well-established privacy and security threats associated with downloading software from KaZaa, Grokster and other "free" P2P software applications.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00207 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.157

The DMCA Balance:

So what do these statistics and Verizon's brochure have to do with the issues being addressed by the Committee today?

First, they help explain why RIAA's members with the support of a broad array of other organizations in the music industry representing artists, songwriters, music publishers, and record stores, took the action we announced yesterday.

Second, and perhaps more important for this hearing, they illustrate that Congress – following the leadership of this Committee -- saw the future in 1998 when it passed the Digital Millennium Copyright Act. The rampant piracy of music on the Internet is a true to life example of exactly the kind of problem Congress envisioned copyright owners would face in the digital world. Although P2P technology did not exist in 1998, Congress understood that the Internet and advances in technology would lead to an explosion in online theft of intellectual property.

Fortunately, at the time, Congress also had the wisdom and saw fit to include in the DMCA a fair and balanced procedure that enables copyright owners meaningfully to enforce their rights in the digital world. The framework established in §512 – commonly referred to as the DMCA information subpoena

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00208 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.158

provision -- ensures that copyright owners, with the help of Internet Service Providers ("ISPs"), have an accessible and efficient mechanism for identifying individuals who are using the Internet to commit piracy.

The balance struck by Congress in §512 was the result of a give and take – in the best sense – between the interests of ISPs and copyright owners, and the need to protect consumers. If you look around, this hearing room is filled with many people – people at the dias, people behind the dias, people at this table, and people in the audience – who spent countless hours discussing and negotiating what became §512. The final product of their efforts represented Congress's recognition that traditional enforcement remedies available to copyright owners were insufficient in an era in which massive amounts of piracy could occur instantly at the hands of anyone with an Internet connection.

Congress also understood that in a digital world, ISPs often would be the sole source for identifying individuals who are engaged in online piracy regardless of the type of technology they were using. So, in exchange for exempting ISPs from any liability for the infringing activities occurring on or over the their networks and connections – subject, of course, to certain prerequisites -- Congress created a framework by which copyright owners, with the assistance of ISPs, could expeditiously identify individuals engaging in infringing activities online. That compromise -- expeditious access for copyright owners to identifying information

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00209 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.159

of infringers in exchange for broad liability limitations for ISPs – is as fair today as it was in 1998.

Keep in mind that absent the broad liability limitations of the DMCA, ISPs could face enormous monetary liability for the actions of their subscribers. With the current levels of piracy, that could translate into enormous monetary liability. That fact helps explain why Judge Bates -- the federal district judge who presided over the enforcement proceedings between RIAA and Verizon -- concluded that: "[i]t would not serve the public interest for Verizon to continue to receive the benefits of the [DMCA] – liability protection – without the concomitant obligations of disclosing the identity of an alleged infringer [under §512]."

Verizon's Privacy Arguments:

Beyond the purely legal, statutory construction questions that have arisen concerning §512, Verizon and other ISPs now contend that there are privacy problems associated with the DMCA information subpoena. Before I address these concerns, it's important to make one thing crystal clear: no one has a privacy right to engage in copyright infringement on the Internet. Despite many novel arguments to the contrary, illegally sharing or downloading copyrighted music online is not a form of free speech or civil disobedience protected by the First Amendment.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00210 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.160

It is also worth noting that during the first-round of litigation in our case, Verizon failed in any way to even mention or raise what they now contend is the biggest issue presented by this case: privacy. Rather than make their arguments in Court, Verizon chose instead to make their case in the court of public opinion.

Only after Verizon lost decisively on its legal arguments in the first-round of litigation did it decide that its privacy-related arguments warranted the Court's attention. The outcome, however, was no different. The district court found Verizon's privacy arguments as uncompelling as its legal arguments. Here is some of what Judge Bates specifically had to say about Verizon's privacy arguments:

- Verizon's customers should have little expectation of privacy (or anonymity) in infringing copyrights. Subscribers to Verizon's Internet services are put on clear notice that they cannot use Verizon's service or network to infringe copyrights.

- [A]s part of its corporate policy, Verizon alerts its subscribers at the outset that it will "disclose" individual customer information to an outside entity...when Verizon is served with valid legal process for customer information.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00211 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.161

- [I]f an individual subscriber opens his computer to permit others, through peer-to-peer file-sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world.

- The [§512 information subpoena] protections ensure that a service provider will not be forced to disclose its customer's identifying information without a reasonable showing that there has been copyright infringement and [t]hese requirements provide substantial protection to service providers and their customers against overly aggressive copyright owners and unwarranted subpoenas.

Although we agree with Judge Bates' reasoning and conclusions, I want to address some of Verizon's privacy arguments in greater detail.

As I understand Verizon's argument, disclosing its subscribers' identifying information (name, address, phone number, and e-mail) pursuant to a valid DMCA information subpoena threatens to violate its subscribers' privacy because the information subpoena process -- in their estimation -- is susceptible to abuse and does not provide the same protections afforded by a more traditional "John Doe" lawsuit. But Congress considered and decided this question back in 1998.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00212 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.162

Ironically, the very principle ISPs profess to defend – the privacy of their subscribers – is at greater risk in a John Doe action than through the information subpoena provisions of the DMCA. There are statutory limits on the type of information a copyright owner can obtain via an information subpoena and the purpose for which that information can be used. Under a DMCA information subpoena, a copyright owner can only receive information that is necessary to identify and contact the alleged infringer – a name, address, phone number, and e-mail. More importantly, the copyright owner is statutorily limited to using that information exclusively for purposes of enforcing their copyright. Compare that to the John Doe alternative where a copyright owner can request anything relating to the ISP's subscriber account, including user habits, website visits, and payment records. Moreover, once that information has been provided to a copyright owner, there are no statutory restrictions whatsoever on how it can be used or to whom it can be shared. This fact makes Verizon's argument all the more suspect.

The information subpoena provisions of the DMCA illustrate that Congress not only understood the importance of protecting the privacy of end users, but also built in specific procedural safeguards designed to protect individuals from unwarranted disclosures of their information. As Judge Bates noted in his decision, the DMCA information subpoena "provides greater threshold protection

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00213 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.163

against issuance of an unsupported subpoena than is available in the context of a [traditional] John Doe action."

The DMCA Information Subpoena Requirements & Safeguards:

As I stated previously, P2P software applications like KaZaA and Grokster are, by design and practice, open networks that enable individual users to search for and copy files located on the hard-drives of other users on the network. By logging onto these open networks and searching for files like any other user, the RIAA is able to identify the Internet Protocol addresses ("IP addresses") of individuals who are illegally uploading or downloading our works. Once we have obtained an IP address and matched that address to an ISP, the information subpoena provision of the DMCA allows us to enlist the help of the ISP in identifying those who steal our works.

Before obtaining any subscriber's information under the subpoena provisions of the DMCA, a copyright owner must provide to the clerk of a Federal district court:

- *A physical or electronic signature of a person authorized to act on behalf of the owner* of an exclusive right that is allegedly infringed.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00214 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.164

- *Identification of the copyrighted work claimed to have been infringed*, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
- *Identification of the material that is claimed to be infringing* or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
- *A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner*, its agent, or the law.
- *A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner* of an exclusive right that is allegedly infringed.
- *A sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title*.

A failure to adhere to any of these requirements is a justification for denying the subpoena and any copyright owner who misrepresents itself in satisfying these requirements is liable for damages, including attorney's fees. With these

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00215 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.165

requirements and safeguards in mind, I want to address some of Verizon's specific arguments.

Anyone who has followed our ongoing litigation has heard Verizon boldly and repeatedly assert – without providing any examples or substantiation – that the DMCA information subpoena process is ripe for abuse at the hands of criminals. It is nothing short of amazing that in an effort to protect its bottom-line, Verizon would repeatedly make such baseless and desperate arguments. The RIAA, the copyright community as a whole and, more importantly, the Members of Congress who crafted the DMCA, would never defend or embrace a procedure that makes it easy for criminals to find victims. Verizon knows this and the public policy debate deserves better.

When I think of this argument, it reminds me of an old law school adage: when the law is not on your side, argue the facts; when the facts are not on your side, argue the law; and when neither the facts or the law are on your side, pound the table. In this case, Verizon risks breaking the table with its argument.

As Judge Bates noted in his second subpoena decision:

- "[I]t is noteworthy that although it has been nearly five years since § 512 came into effect, there is nothing in the record to indicate that the DMCA

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00216 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.166

subpoena authority has been used for stalking or other fraudulent purposes."

- "Verizon's bald speculation of mistakes, abuse or harassment that has yet to occur to any degree (let alone to any substantial degree) since the statute was enacted is simply not enough,...[and] requirements in the DMCA should prevent such speculation from ever becoming a reality."

On a more practical level, however, Verizon's arguments simply don't hold water. Few, if any, criminals are willing to pay money and appear in Federal Court to identify themselves and leave a trail of information for authorities to follow. And even assuming a pedophile were willing go through the hassle of obtaining an anonymous IP address, forge a series of documents establishing his status as a copyright owner, and risk his own anonymity by appearing in Court, he can only obtain the adult ISP subscriber's contact information – and not any information relating to a child.

A cyber-pedophile looking for victims online is much more likely to get what he wants by simply sending an instant message to the unwitting young person who downloads an Olsen twins or pokemon file from the pedophile's share folder on KaZaa. And for the domestic abuser who already knows the identity of his victim, it's even harder to imagine that with all of the different ways to track someone

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00217 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.167

down that he'd subject himself to the hassles and risks of the DMCA information subpoena process.

The facts and common-sense make clear that the cyber-pedophile and domestic abuser scenarios put forward by Verizon are little more than legal and public policy strawmen.

John Doe Lawsuits as an Alternative to Information Subpoenas:

Another argument put forward by Verizon is that requiring copyright owners to file a John Doe action in Federal Court will in some way provide greater privacy protections to its subscribers. In fact as discussed earlier, requiring copyright owners to file John Doe lawsuits would provide fewer protections to an ISP's subscribers, while effectively depriving copyright owners of expeditious access to an alleged infringers' information – exactly what Congress intended to provide copyright owners through §512. .

Not surprisingly, for ISPs, the John Doe approach is a win-win: they retain their broad liability limitation, while making it more difficult for copyright owners to obtain information – despite the fact that online piracy is skyrocketing. In stark contrast, for copyright owners, the John Doe procedure is a lose-lose: they no longer have access to an expeditious procedure for identifying alleged infringers

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00218 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.168

and they are faced with significantly greater administrative and monetary burdens associated with enforcing their rights under the law. It's not hard to see why ISPs think this approach is better.

ISP Notice to Subscribers:

The RIAA and the copyright community as a whole understand the interest of the Committee and Congress as a whole in protecting the privacy of individuals. In the context of the DMCA information subpoena process, we also believe that protecting individual privacy reasonably and effectively already can be achieved through ISPs providing notice to their subscribers as soon as information is turned over to a copyright owner pursuant to a valid DMCA subpoena. In fact, nothing prevents ISPs from institutionalizing the practice of notice. The benefits of such a policy are clear --

- the subscriber is made aware that their information (name, address, phone number, and e-mail) has been turned over at the same time it's being given to a copyright owner pursuant to a valid information subpoena;
- the subscriber knows both who the information is being turned over to -- further helping to prevent any potential abuses of the process – and is made aware of the allegations warranting the disclosure;

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00219 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.169

- the subscriber is given an opportunity, in a timely manner and before any formal action is taken, to contact the copyright owner if the subscriber believes that the allegations underlying the subpoena are mistaken;
- the subscriber who is engaging in activity (other than piracy) protected by the First Amendment has an opportunity to contest the actions of the entity receiving the information.

The benefits of notice go a long way toward resolving any – perceived or real – privacy problems associated with copyright owners using the DMCA information subpoena. And when combined with the statutory use restrictions placed on copyright owners who obtain information under the subpoena provisions, we believe it is clear that no change in the law is needed.

Conclusion:

The copyright community believes that the DMCA information subpoena represents a fair and balanced process that includes important and meaningful safeguards to protect the privacy of individuals.

Thank you for the opportunity to testify today and I look forward to answering the Committee member's questions.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00220 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.170

Statement of Thomas J. Spota, Suffolk County District Attorney

Thank you Mr. Chairman and members of the committee. I appreciate the opportunity to come before you this afternoon to discuss the issue of child pornography on peer-to-peer file sharing networks and the efforts of those of us in Suffolk County to combat what we view as a growing concern for law enforcement nationwide.

Earlier this year I was so disturbed by information brought to my attention about the nature and accessibility of child pornography on peer-to-peer networks that I authorized the commencement of an investigation by members of my staff into KaZaA, a popular file-sharing program. I was amazed that the file sharing programs used by so many of our children and adolescents to download music were also the repository of some of the most graphic child pornography available today.

There is no special code or unique search term required to unlock the key to child pornography in these networks. If you search for songs by artists as popular as Brittany Spears or the Beatles, if you are looking for any song with the word "young" as a part of its title, your search results will include child pornography. The names of the files are disturbing enough; a simple click of the mouse is all that is necessary for anyone, including our children, to be exposed to the dark, disturbing and violent world of child sexual abuse.

Working in conjunction with the entire staff of the Suffolk County Police Department Computer Crimes Section the investigation conducted by my office relied upon sophisticated computer technology and good old-fashioned police work. Numerous grand jury subpoenas were issued to Internet service providers. Search warrants were executed and computers, cd's and other storage medium were seized. Police officers who are also forensic computer analysts evaluated the seized evidence and recovered hundreds of images of child pornography.

Upon the completion of the forensic analysis, evidence was presented to a grand jury that resulted in the indictment of eleven Suffolk County residents' for over 180 counts of the possession and promoting of child pornography. The defendant's range in age from 16 to the mid 40's and include a college student using a laptop computer and a chemist for a major cosmetics company. They are fathers, brothers and in one instance a young woman living with her grandparents.

The images of child pornography available on peer-to-peer networks are some of the worst seen by law enforcement to date. Included in the images seized by police in the cases being prosecuted by my office, are still photographs of very young children engaged in sexual acts with other children and adults and video clips lasting several minutes of children being subjected to unspeakable acts of sexual violence. Some of these video clips have sound and in one case a child can be heard screaming, "No daddy, stop, no daddy" in a futile effort to prevent a rape. To say that this is disturbing is an understatement.

93014.171

Contrary to the assertion of some, child pornography is not a victimless crime. Not only does every image represent the sexual assault of a helpless child, the use of a medium such as the Internet or a peer-to-peer network allows the assault to be broadcast worldwide and re-victimizes the child each and every time that the image is viewed. Today, it is not uncommon for a child to report that their abuse has been recorded and later for the images to turn up in the forensic examination of a computer in a totally unrelated case. Thus, this child's abuse will be available forever on the Internet or on a peer-to-peer network. How devastating this must be for a child, to know or come to understand that your victimization is available to the world in perpetuity.

The government must act to make peer-to-peer file networks responsible for the child pornography available to their users. Law enforcement activities can serve to punish offenders and educate the community but they will never be enough to ultimately stem the tide. The profit must be taken out of the business of sharing child pornography for the operators of these networks.

The government must do more to educate and inform American parents. Seasoned child abuse prosecutors in my office and elsewhere were unaware of the capability of KaZaA to file share child pornography until they undertook my directive to begin this investigation. How many other parents are unknowingly putting their children at risk by allowing them access to a program they believe is harmless? Americans employ a rating system for movies and TV shows to protect children. Compact discs contain parental advisories. KaZaA and programs like it do not contain such warnings. This is wrong.

As far as I am aware I am the only District Attorney to investigate and prosecute users of a peer-to-peer file-sharing network for the possession and promotion of child pornography. This case has generated considerable interest from other law enforcement agencies and I hope that they will initiate additional prosecutions. Our investigation is also continuing in the hopes of identifying some of the perpetrators of these horrific acts and the children so that they can be protected from further abuse. As is standard protocol in these cases the images will be forwarded to the National Center for Missing and Exploited Children to aid us in this endeavor.

Thank you again for inviting me to address the committee on this important issue. I will be happy to answer any questions members may have.

93014.172

INDECENT EXPOSURE: OVERSIGHT OF DOJ'S EFFORTS TO PROTECT PORNOGRAPHY'S VICTIMS

WEDNESDAY, OCTOBER 15, 2003

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 2:11 p.m., in Room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, Chairman of the Committee, presiding.

Present: Senators Hatch and Grassley.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Chairman HATCH. Good afternoon. Today, we will be conducting an oversight hearing on the Department of Justice's efforts to prosecute child pornography and obscenity.

As many of you know, pornography is a growing problem in America. For example, in a recent "ABC Primetime Thursday" story, Diane Sawyer stated that the pornography industry is estimated at $10 billion, which is bigger than the NFL, NBA, and Major League Baseball all combined. And it is getting worse with the advent of the Internet. Pornographic web pages now number 250 million—250 million—and are growing at an unprecedented rate. It is estimated that porn on the Internet will grow to become a $7 billion—that is with a "B"—billion dollar industry in the next 5 years unless we have aggressive law enforcement.

The National Society for the Prevention of Cruelty to Children estimates that there are 140,000 images of child pornography online. The typical age of children depicted in these images is between six and 12, but the profile is getting even younger.

In addition, adult pornography has become readily available to minors. There are currently 28 million children and teenagers with access to the Internet and an additional 50 million globally are estimated by the year 2005. Nine out of ten children, ages eight to 16, have viewed pornography online, most of them unintentionally and when using the Internet to do their homework. And those children who seek it out of curiosity have absolutely no difficulty or trouble getting it. Ninety-seven percent of adult websites do not require adult verification.

The result of all this porn is that there are 11-, 12-, or 13-year-old children being treated for pornography addiction. As Professor Victor Cline previously testified before the Child Online Protect

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00223 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

Act, Commission, or COPA, the overwhelming majority of pedophiles use child pornography to simulate and whet their sexual appetites before abusing children. They also use child porn to desensitize children and lure them into participating in sexual activity. In addition, as the "ABC Primetime Thursday" piece made clear, the victims of pornography are not just addicts and rape victims, but young, innocent teenagers who go to Los Angeles with dreams of becoming a movie star and instead get caught up in this sordid industry.

I have always believed very strongly in protecting children from this type of offensive material. I sponsored the PROTECT Act, which the President signed into law 6 months ago. This is one of the most significant pieces of child crime legislation that Congress has passed in decades. It gives law enforcement the tools it needs to effectively prosecute child pornographers. In addition to authorizing criminal prosecutions of child pornographers, the Act provided funding for more prosecutors and investigators and established a cyber tip line to report online child exploitation. It also created a national registry of child pornographers.

I am currently considering legislative solutions to the many risks inherent in the use of peer-to-peer networks. Almost half of the people who use peer-to-peer networks are minors. Recent studies have shown that millions and millions of pornographic files are available for downloading on these networks at any given time. Even more disturbing is that searches on these networks use search terms that a child would be expected to use, such as Harry Potter or Pokemon, and they turn up an enormous percentage—over 50 percent in one study according to the GAO—of pornographic materials, including child pornography. Now, this is simply unacceptable.

Many parents, possibly the majority of them, are unaware of this problem, and I think this requires our immediate attention.

I look forward to hearing about DOJ's efforts to combat both child pornography and obscenity. This is a growing problem that we need to attack aggressively. We cannot sit quietly and hope that this whole set of problems is going to go away.

The hearing today will consist of two panels. The first panel includes three representatives from the U.S. Department of Justice, John Malcolm, Deputy Assistant Attorney General of the Criminal Division; J. Robert Flores, Administrator of the Office of Juvenile Justice and Delinquency Prevention; and Mary Beth Buchanan, U.S. Attorney for the Western District of Pennsylvania. In addition, we have Lawrence Maxwell, Inspector in Charge from the Postal Inspection Service.

The second panel consists of Bruce Taylor, President and Chief Counsel to the National Law Center for Children and Families; Detective Steve Takeshita, Officer in Charge of the Pornography Unit in the Los Angeles Police Department; and Emeritus Professor from the University of Utah, my own friend, Dr. Victor Cline, who, of course, is one of the great experts in this field and child psychiatry.

Welcome to the hearing. I want to welcome all of you and I look forward to listening to your testimony.

In addition, at this time, I would like to submit for the record the written testimony of Donna Rice Hughes, President of Enough is Enough, an advocate of protecting children from pornography on the Internet.

[The prepared statement of Senator Hatch appears as a submission for the record.]

Chairman HATCH. We will start with you, Mr. Malcolm. We will take your statement first and then just go across the table.

STATEMENT OF JOHN G. MALCOLM, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. MALCOLM. Thank you, Mr. Chairman. I thank the Committee for inviting me to testify about the Department of Justice's enforcement efforts against those who produce and disseminate adult obscenity and child pornography.

In addition to pornographic material, which is constitutionally protected, adult obscene material and child pornography, which are not constitutionally protected and which are illegal, are unfortunately pervasive in our society. While there is no doubt that the Internet provides access to a highly diverse network of educational and cultural content, it is also responsible for the proliferation of adult and child pornography and obscene material.

Indeed, offensive material that used to be largely unavailable to average citizens and children is now largely unavoidable. Offensive material is readily available to anyone with an Internet connection, accessed oftentimes by unsuspecting children and adults who had no intention to seek such material and no desire to view it.

The proliferation of this material and the desire by pornographers to differentiate themselves in a highly competitive market prompted pornographers to produce ever more offensive material. In addition to child pornography, pornography depicting and glorifying bestiality, scatology, and rape are readily available and aggressively marketed.

The harmful effects of obscene material and the victims of this sordid industry are very real. The images produced promote the idea of sex without consequences, such as unwanted pregnancies or sexually-transmitted diseases. The victims, usually women, are objectified and demeaned, presented and completely nondiscriminating with respect to the number of type of sexual partners they have and as being aroused and gratified by being beaten, tortured, or raped.

Very few women grow up dreaming of being filmed having sex with an animal or being raped and beaten by multiple partners, and very few who see these powerful images and absorb the antisocial values they portray can remain unaffected by them. The negative lasting impact that this has on the participants who are in these images and on the attitudes that are formed by the predominately male viewers who see them is incalculable.

The negative impact and effects of child pornography, while more readily apparent and universally recognized, are too horrifying to think about. Images of young teenagers, prepubescent youngsters, and literally infants engaging in sex of all types with other children

and adults are readily available and would make you sick to your stomach.

As well, pedophiles frequently use child pornography and obscene material to lower the inhibitions of their victims and to persuade them that adult-child sexual interaction is perfectly acceptable. Too often, this pernicious ploy works.

Attorney General Ashcroft publicly stated that the Department is unequivocally committed to the task of prosecuting obscenity. Since that time, attorneys with the Child Exploitation and Obscenity Section, CEOS, which I oversee, working with prosecutors and U.S. Attorneys' offices around the country, have created an obscenity enforcement strategy and have made tremendous progress in combatting the scourge of obscenity.

In order to aggressively and effectively combat the online distribution of obscenity, the Department created the High Tech Investigative Unit. This unit is staffed with computer forensic experts who bring their special technological expertise to bear against Internet-based child pornography and obscenity offenders, many of whom feel impervious to law enforcement because of the perceived anonymity offered by the Internet. Working side by side with CEOS trial attorneys and Federal agents, these computer forensic specialists meet the challenges presented by the use of emerging Internet technology and are poised to meet new challenges that will surely develop as technology evolves.

CEOS also conducted a symposium on obscenity in June 2002 to discuss strategy. The Attorney General personally addressed the audience and, via live simulcast, U.S. Attorneys' offices throughout the country. In October 2002, CEOS presented an obscenity training seminar and a second annual obscenity training seminar began today and will last the rest of the week. Through such training, the Department hopes to develop a framework for sustained long-term enforcement of Federal obscenity laws to complement the anti-obscenity efforts of State and local prosecutors and investigators.

I am pleased to state that the Department's efforts are starting to bear fruit. To date, during this administration, there have been 19 convictions involving Federal obscenity statutes. Two defendants, including a former police officer who allegedly distributed rape videos, are on trial right now in Federal court in Dallas, Texas. Two other cases of large-scale distributors of allegedly obscene material have been indicted, and approximately 50 Federal obscenity investigations are ongoing at CEOS and in districts throughout the country.

While the Department is committed to a renewed enforcement agenda with respect to adult obscenity, and despite the obvious drain on resources by the war on terrorism, the Department continues to vigorously enforce child sexual exploitation laws. Indeed, according to the Executive Office of U.S. Attorneys, in fiscal year 2002, 1,199 cases were filed, a 22 percent increase over the previous year.

Internet investigations often uncover large child pornography groups with hundreds and sometimes thousands of targets. The Internet affords the pedophiles the ability to communicate with a large number of people with minimal effort. CEOS is currently involved in nine national significant operations. We work very closely

with the U.S. Attorneys' offices and with the Internet Crimes Against Children Task Forces, and I am proud to say that though these operations are ongoing, several active molesters have already been caught and convicted and several children have been identified and rescued.

Mr. Chairman, we are under no illusions that this task is going to be easy or that we are not going to face challenges in the future. Nonetheless, the Department of Justice will do everything within its power to curb the proliferation of obscene material in our society and to protect children, both at home and abroad, from the predatory activities of pedophiles. Thank you.

Chairman HATCH. Thank you.

[The prepared statement of Mr. Malcolm appears as a submission for the record.]

Chairman HATCH. Mr. Flores, we will turn to you.

STATEMENT OF J. ROBERT FLORES, ADMINISTRATOR, OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION, OFFICE OF JUSTICE PROGRAMS, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. FLORES. Mr. Chairman, I am Bob Flores, the Administrator of the Office of Juvenile Justice and Delinquency Prevention. On behalf of the Department, I am grateful to have an opportunity to testify today on the subject of protecting the victims of pornography.

The office that I head continues to commit resources to protect children and families from the harms associated with sexual exploitation, sexual abuse, child pornography, and sexual predators. Historically, OJJDP has provided that assistance through its administration of funds, technical assistance and training, as well as information that we distribute and disseminate to the public at large. I want to assure you the commitment has never been stronger, and as I will detail for you, is being expanded to provide the help you seek for children and families, and that the President and the Attorney General are publicly committed to providing.

OJJDP has been involved with tackling the child pornography and computer facilitated child sexual exploitation problems since 1998, when the first ten Internet Crimes Against Children task forces, or ICAC task forces, were identified and funded. Last year, the President sought and obtained from Congress additional funding to assure nationwide coverage and the task forces now number 40, but we expect by the end of this year to bring the number up to 45. They provide regional assistance. They are made up of Federal, State, and local technical and investigative experts and offer prevention and investigative services to children, parents, educators, law enforcement officers, and others working on these issues.

We recognize that the increasing online presence of children, the proliferation of child pornography, and the lure of predators searching for unsupervised contact with children, represents a significant threat to the health and safety of our families and a formidable challenge for law enforcement today and into the foreseeable future. There is a tremendous amount of work, however, that has already been done. We have been working together with the Depart-

ment's Criminal Division and with other departments. I have also brought this matter to the attention of the Coordinating Council on Juvenile Justice and Delinquency Prevention, which now has a Technology Subcommittee.

The ICAC task forces alone have been responsible for over 1,500 arrests in the past 5 years, with nearly 500 of those taking place in just the past 12 months. In addition to these arrests, the ICAC task forces have made nearly 2,600 case referrals to non–ICAC law enforcement agencies. Of the 14,000 cases the ICAC task forces have been involved in over the past 5 years, either through actual investigations, referrals, or technical support, nearly 11,000 of those have been directly related to the possession, distribution, or manufacturing of child pornography.

What are the next steps, however? Children are still at significant risk of exploitation. Much of the government's efforts have been focused on investigation and prosecution after the act of exploitation has occurred. For that reason, the Department, at the direction of the President and the Attorney General, is expanding the traditional efforts to include a focus on prevention, and cleaning up the cyber environment in which our children and families learn, play, and work.

OJJDP will contribute to this effort by targeting the distribution of obscene material to children. This alarming trend has a two-fold impact. First, as noted previously, while predators use child pornography to recruit, seduce, and control future victims, they also often use adult pornography and obscene material, as well as material harmful to minors, to break down a child's barriers and desensitize them as a means to lure and seduce them into abuse.

Secondly, the distribution of obscene material to children is the commercial porn industry's vehicle, intentional or not, to create a new generation of pornography junkies. Some children are drawn to the commercial websites through the manipulation of common and well-known children's website names. Other children encounter this as a result of pornography's pervasive presence on the Net. We must address not only the predators and the exploiters, but we must also address those who help create the atmosphere in which children and families who use the Internet are deluged by illegal and unwanted pornography.

Today, Senator the Internet is so polluted that it is difficult to pick out a single item of garbage. Moreover, as the pornography morass has grown, it is now much easier for a predator to find a place to hide amid the garbage. The decision to allow Internet pollution to grow, and with it the sense that anything goes, has cost our children a great deal. Thus, we must begin to look at the illegal activity on the Internet as a whole, and send a clear message that the law does apply to this critically important medium and that we will not abandon it to those who would abuse it.

In response to this, I have directed the ICAC task forces to include, as part of their investigative effort, a new focus on adult obscenity cases when a child is the target of the material; or if such material has been used to seduce or facilitate the exploitation or abuse of a child.

In addition to this, it is important to make sure that the community at large is educated, if we are to have hope that we can actu-

ally change the culture on the Internet. This pertains not only to the child pornography issue, but to responsible use of the Internet, including issues that are as important for industry as they are to any family—the theft of intellectual property and copyright materials.

One of the efforts that we are going to launch is the erection of a comprehensive education and prevention strategy. We have already taken the first step in March of this year by having a meeting where we brought together government as well as private entities, agencies, and organizations. We will continue in November as we meet together and again and really focus on what is necessary to create a strategy that doesn't depend just on the Justice Department, but includes the Health and Human Services Department, the Department of Commerce, the Department of Labor, and the Department of Education. Each of the departments has a role to play. I look forward to an opportunity to report back to this Committee and to keep your staff informed as we continue.

I have great confidence that we can succeed at this point in time because we stand in a different place now than we did a year ago. Corporate America has recognized, perhaps in a way it wished it did not, that an environment of lawlessness and an inability of Internet users to properly translate how law operates in the real world to the cyber world, jeopardizes their existence. Parents have come to understand this through tragedies.

I am encouraged that we are here and that much progress has been made. I look forward again to having an extended conversation with your staff, and I am pleased to take any questions that you may have.

Chairman HATCH. Thank you, Mr. Flores.

[The prepared statement of Mr. Flores appears as a submission for the record.]

Chairman HATCH. We are going to interrupt for a second here. The distinguished Chairman of the Finance Committee would like to make a statement, and we will turn to Senator Grassley at this time, and then I know that he has to leave a little early because of the Medicare prescription drug conference that both of us are supposed to be to. But he is going to carry the banner for me over there this afternoon.

Senator Grassley?

STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. I am very happy to have your cooperation so I can appear for a short period of time at this hearing, because I have been very much interested in this going back to the Farber Act a long time ago, in the mid–1980's, I believe it was. But most importantly, Mr. Chairman, thank you very much for your interest in this over a long, long period of time, as well, probably before my involvement in it, and your continuation through this hearing.

Hardly a week goes by that I don't receive a letter from an Iowan concerned about pornography and its harmful effect on family. My constituents want to know what the government and the Congress are doing about all the smut that invades their homes by way of the Internet and cable television. So I want you all to know, and

particularly you, Mr. Chairman, that I appreciate this hearing because it is a partial answer to my constituents' concerns.

It seems that since the mid–1990's, Congress has made some valiant attempts to pass constitutional protections for children using the Internet. So far, we have a mixed record. The Supreme Court has overruled one of our bills, the Communications Decency Act, which tried to protect children from indecent material on the Internet. It upheld one, the Children's Internet Protection Act, which requires public libraries and schools to install Internet filters. And just yesterday, the Court agreed to take up another case, the Child Online Protection Act, which, if upheld, and I am optimistic that it will be, will shield children from material that is, according to the law, quite, "harmful to minors" while they surf the Internet. I supported each of these bills and I am very glad that we could get them passed.

During the last 10 years, the obscenity and child pornography industry has grown at quantum leaps. It is no coincidence that during the same time, the Department of Justice did precious little in the area of obscenity prosecution. By all accounts, the Clinton Justice Department brought no more than a handful of obscenity prosecutions, and I am forced to believe that that sort of laxity towards this area of Federal criminal law has contributed to the "Wild West" environment that we have on the Internet.

Unfortunately, some have been critical of the current administration for being slow out of the gate with regard to the enforcement of these obscenity laws. I don't know whether this is the case or not, but I am very happy that the Department of Justice can be here today to discuss their efforts. It is my understanding that the investigation and prosecution of these crimes is complex and time consuming and is further complicated when the Internet is used to distribute this obscene material.

In reviewing the testimony, I was particularly glad to hear about the Office of Juvenile Justice and Delinquency Protection's Internet Crimes Against Children task forces that are very important, it seems to me, to leverage State and local resources in the effort to protect children from obscenity as well as child pornography.

There is substantial evidence that obscenity is not a victimless crime. According to a report of the Child Online Protection Act Commission, obscenity is a tool used by molesters in child molestation and exploitation. I also agree with Administrator Flores in his assertion that the distribution of obscenity, especially on the Internet, target children with deceptive-sounding website names so that they may reach their next generation of users. The illegal child industry is big, big business and our children are paying the greatest cost of these criminal commercial successes.

Because of the harm that obscenity poses for minors, it is critical that the ICACs be given technical assistance and training in how to investigate and prosecute Federal obscenity crimes as well as child pornography. By arming State and local investigators and prosecutors, we will be enlisting an army in an effort to protect women and children from this sort of exploitation.

So once again, I thank you, Mr. Chairman.

Chairman HATCH. Thank you, Senator Grassley. We appreciate having you here and appreciate the hard work you give us on this

Committee and we appreciate your very, very strong interest in this area and finding solutions to these problems, so we appreciate having you here.

Next, we will turn to you, and then we are going to wind up with our U.S. Attorney for the Western District of Pennsylvania.

STATEMENT OF LAWRENCE E. MAXWELL, INSPECTOR IN CHARGE, FRAUD AND DANGEROUS MAIL INVESTIGATIONS, POSTAL INSPECTION SERVICE, WASHINGTON, D.C.

Mr. MAXWELL. Thank you, Chairman Hatch. It is an honor for me to be here representing the Postal Inspection Service. I have prepared a written statement, which I would like permission to submit to the record.

Chairman HATCH. We will put all written statements in the record as though fully delivered, and any additional comments you would care to make that you would care to augment the record with.

Mr. MAXWELL. Yes. I would like to just make a few comments, first of all to acknowledge my associates here at the table. Truly, this is a team that sings from the same page of music. We have for years. Mr. Malcolm provides the leadership and the direction for law enforcement to get along and to focus on the strategy. Mr. Flores, we have worked with for many years and his oversight with the juvenile programs and especially the ICAC task forces have been very instrumental. It is a very difficult task for him to pull all those different factions together and he has done it tremendously. The lady to my left, she is known to our agency as a tremendous advocator for law enforcement. She is a tremendous prosecutor and we have had a lot of experience with her, as well, and I will let her tell her story in a few minutes.

The Inspection Service, and I know you know us well and I know your support goes far and deep. I have seen you at the May Congressional breakfasts. I know you take the time to come and honor the agents there. The Inspection Service itself, we go back, we trace our roots to our founder, Benjamin Franklin, and we are tied into that American institution, the Postal Service, which visits every home. So we have an overriding responsibility and passion to protect the Postal Service because in doing that, it protects the American public.

Our mission has changed a lot over the years, but its primary focus hasn't changed. We have roughly 200 statutes which we now enforce, limited to Postal violations. However, we don't stop because the mailings stop. We help our brethren in law enforcement to continue those investigations.

In the cases of pornography, obscenity, I am proud to say that Anthony Comstock, who was a Postal Inspector in 1873, and he was the first to draft language for legislation which became the forerunner—it was the Comstock Act and it became the forerunner of 1461, which we utilize today. We were proud to be the first to enforce that law.

As we enter this century and we see the evolution change of mail to Internet, still a large part of our cases focus from Internet solicitations. In fact, what we have seen, in 1997, 33 percent of our cases originated online, solicitation followed by some form of mailing.

Today, we see 70 or more—considerably more at certain times—originating on the Internet. So we have a concern that things have changed dramatically and we need to keep our enforcement capabilities changing with them and we are striving to do that.

Throughout the different legislative enactments, from the Sexual Exploitation of Children Act, the Child Protection Act, which gave additional teeth to trafficking not only for profit. When it became online, we had several cases that blossomed from those online solicitations and one in particular was called Operation Avalanche, which you may be familiar with. It was worked with the Dallas Police Force and the ICAC task force.

The case itself had tremendous implications and it was the farthest reaching at the time of an Internet provider of child exploitation materials. It has reached to date globally with 4,000 sites being searched. What I have seen, from my standpoint, it has raised the level of awareness internationally that this is a problem that is global. It is not just restricted to the United States. We now need to focus on our partnerships with those law enforcement agencies and those governments.

Since 1997, 257 child victims have been identified and rescued. Since the enactment of the Child Protection Act in 1984, Postal Inspectors have arrested and prosecuted more than 4,000 child molesters and pornographers. We find many, if not most, of the pornographers are indeed molesters, as well.

Finally, in focusing on adult obscenity, that would fall to a lesser extent of an effort because we are focusing so heavily on child exploitation with limited resources. The Inspection Service, unlike our counterparts, is not appropriated. We are funded by rate payers' money, so we are limited in terms of our growth potential, but we do a lot with less. We have roughly 50 agents that focus on child obscenity—adult obscenity and child exploitation and those accomplish all of that.

Having said that, our counterparts, our partnerships are very valuable to us as we proceed. Most recently, we have focused on Extreme Associates in Pittsburgh, which was prosecuted by Mary Beth Buchanan's district, which shows the length and breadth that this adult obscenity has expanded to on the Internet. And you will be happy to note that we were the very first to apply your PROTECT Act legislation in a case in New York, where we prosecuted the individual who sold, I think approximately three million in licenses for domains.

Chairman HATCH. You are going to give us a lot of illustrations how we might even improve on the PROTECT Act?

Mr. MAXWELL. Correct.

Chairman HATCH. Although I think we gave you an awful lot of law enforcement tools with that.

Mr. MAXWELL. You did. You did. It has been excellent.

Chairman HATCH. That is one of the most important Federal anti-crime statutes that we have had the whole time I have been here.

Mr. MAXWELL. And it couldn't come at a better time, because right now, that is what we are seeing in terms of where they are using it.

Chairman HATCH. Good. We would love your advice on it.

Mr. MAXWELL. Okay. Anyway, I thank you for your time. I am here to answer any questions.

Chairman HATCH. Thank you so much.

[The prepared statement of Mr. Maxwell appears as a submission for the record.]

Chairman HATCH. We are delighted to have you, Ms. Buchanan. You have a great reputation and graduated from my alma mater, as well. I think that just makes it even better. So we are happy to have you here.

STATEMENT OF MARY BETH BUCHANAN, UNITED STATES ATTORNEY, WESTERN DISTRICT OF PENNSYLVANIA, PITTSBURGH, PENNSYLVANIA

Ms. BUCHANAN. I hope you are not feeling as badly as I do about Pitt's loss to Notre Dame.

[Laughter.]

Chairman HATCH. Well, I have always rooted for both schools, to be honest with you.

Ms. BUCHANAN. Well, thank you, Mr. Chairman. It is an honor to appear before you today on behalf of my office and on behalf of all of the United States Attorneys around the country who are involved in prosecuting cases of child pornography and obscenity.

Before my appointment as the United States Attorney, I served as an Assistant United States Attorney for 13 years and I specialized in the area of prosecuting child sexual exploitation cases. In that capacity, I prosecuted many predators who had a sexual interest in children. During the course of my work, I saw that the nature of the cases in this area changed dramatically.

Initially, these cases involved individuals who tried to obtain child pornography through the mails, usually in a very unsophisticated manner. The activity of the predators has evolved during the 1990's to include cases targeting adults who use the Internet not only to trade child pornography, but to meet children and to engage in actual molestation of the children.

With respect to obscenity cases, much has also changed in that area, as well. The adult bookstore has largely been replaced by thousands of websites advertising and selling pornography. Nearly everyone who has received unwanted and offensive spam and e-mails advertising graphic sexual materials understands what I mean. Pornographic websites also offer video tapes, streaming video, and live webcam activity, all of which can be accessed immediately by the computer user. Effectively, this means that the world's worst adult bookstore can now be accessed in anyone's home who has access to a personal computer, and it is not a leap of logic to assume that young people are accessing this material, as well.

The work of the Department of Justice to provide a safe America for children now extends well beyond the physical world into the electronic universe of cyberspace. While the Internet has many great educational benefits, there are also dark corners of the Internet where children are being exposed to inappropriate sexual material. Protecting children is the most important reason to vigorously enforce both our child exploitation and obscenity laws.

I would like to talk about some of the cases that we have prosecuted in Western Pennsylvania. Several years ago, I prosecuted an Arizona minister who had befriended a 13-year-old boy online. Initially, he began sending this boy child pornography. Eventually, he sent him a Polaroid camera and asked the boy to take a picture of himself and to send that picture to the minister in Arizona. Postal Inspectors organized a search of the minister's house and they found boxes and boxes of child pornography, videotapes, and magazines.

In another case just this year, the FBI received information that a Pittsburgh man had been attempting to trade child pornography with an undercover detective in Chicago. A search warrant for child pornography was executed at a residence in Pittsburgh and located at the scene was a 10-year-old girl who had been adopted by this man in Russia for the purpose in engaging in illegal sexual activity with her. This child had been adopted at the age of five and brought to the United States. Images of the child were taken and then placed online by this individual. He recently plead guilty and is facing a sentence of 15 to 20 years in prison.

In another case, a defendant was convicted of possessing child pornography in Los Angeles. That defendant agreed to cooperate with law enforcement and he told law enforcement about a man in Pittsburgh who had been engaging in sexual activities with his own 5-year-old daughter and then showing those activities through a video camera to others on the Internet. This individual even sold his daughter's undergarments to individuals in exchange for child pornography. He was convicted and is serving 9 years in prison. Under the PROTECT Act, the activity of this person would have netted a 25-year sentence, but unfortunately, the conduct occurred prior to the enactment of the PROTECT Act.

All of these individuals possessed thousands of images of child pornography, revealing their strong interest in sex with children. Unfortunately, these perpetrators don't just stop at looking at pictures. They have actually acted upon their perverse sexual interests.

As the extensive nature of the child pornography collections that we have seen reveals, perpetrators are collecting more and more material. They are creating a market and a demand for child pornography, and what this means is the more they collect, the more they want to collect and the more children are going to be victimized in order to make these depictions. And each time that this depiction is shown, the child is revictimized over and over again.

Most recently, we prosecuted a man from Virginia who identified himself on the Internet as the "Master of Teen Slave Girls." He engaged in chat conversations with a 13-year-old girl from Pittsburgh, and on New Year's Day 2002, he traveled to Pittsburgh and transported her to his house in Virginia, where he chained her to a room and intended to make her his sex slave. He had an entire room of torture implements that he intended to use on this child. Fortunately, we were able to utilize the provisions of the PATRIOT Act. Specifically, we used the pen register and trap and trace application and national service provisions to locate the child and we were successful in finding her after only about a day and a half.

Chairman HATCH. Something you didn't have before the PATRIOT Act.

Ms. BUCHANAN. That is absolutely correct.

Chairman HATCH. I get so sick of these people that have no conception of what is in the PATRIOT Act, mostly these journalists who write about it, and yet you have tools now that you should have had years ago but we were stopped by both the far left and far right from giving you but are really making a difference for our families today. I appreciate your bringing that up.

Ms. BUCHANAN. Thank you. Had we not had those tools, we may not have been as successful in locating this child as quickly as possible and the results could have been very different than they were in this case. This particular defendant plead guilty and he will be serving more than 20 years in prison for his crimes.

In these cases and in many others, we have found that there is a direct link between adult and child pornography and the offenders who actually molest children. Images now available on the Internet are more graphic, involve younger children being molested, and increase every day. There are few, if any, crimes that are more serious than the rape of a child. United States Attorneys around the country have placed a very high priority on catching and prosecuting these offenders, and we work very closely with the Child Exploitation Section and all forms of Federal and State law enforcement. The importance of cooperation among all levels of law enforcement is certainly recognized by all U.S. Attorneys.

In Western Pennsylvania, we have formed a Crimes Against Children task force that brought together not only Federal, State, and local law enforcement, but medical professionals and victims' service agencies so that we could address the full needs of the child victims of these types of crimes, and we have found that that has been a very effective tool for us in maximizing the number of prosecutions that we are able to bring and in making sure that all of the needs of the child victims are met.

And before I conclude, Senator, I would like to briefly discuss adult obscenity, because it is important to recognize that adults as well as children can become the victims of pornography. With a CEOS trial attorney, my office recently prosecuted an obscenity case involving Extreme Associates and its owners, Robert Zicari and Janet Romano. Extreme Associates is a California company that has produced some of the most vile, offensive, and degrading material that is available on the Internet.

One of the videos that is being charged, called "Forced Entry," is a series of rape scenes and killing of three women. The women are hit, slapped, and spit upon. Another movie involves sexual acts with multiple men, followed by the women being forced to drink almost every form of bodily excrement. Although the third video apparently involves actresses who are over the age of 18, these women are dressed as children younger than 18. In one of the scenes, the woman is wearing Pokemon pajamas and she is being forcibly raped by a magazine salesman.

Obscenity by its very nature reduces human beings to sexual objects. Just last week, I received a letter from a woman whose daughter had participated in the production of pornographic films. The mother described how her daughter had become a drug-ad-

dicted participant of these obscenity videos. Prior to that, she had been a graduate of a very well-known high school. She had a very promising future, but she got involved in the obscenity industry and this mother, with nowhere else to turn, asked me to do whatever I could to make sure that no other child is victimized the way her daughter was.

I thank you for giving us the opportunity to speak to you today about the problems involved with child pornography and obscenity and I welcome your questions.

Chairman HATCH. Well, thank you. I want to thank you for the work that you have done. A lot of people don't know what you are talking about when you talk about pen register, trap and trace that we now have given you the authority to use under the PATRIOT Act, and that is being able to get the phone numbers into a phone and out of the phone of terrorists or criminals like this terrorist was against this young girl. You would think that was a given. You would think, no way that law enforcement wouldn't have those tools, but we could never get them through. And I was the author of the 1996 anti-terrorism effective death penalty act when we were trying to get laws like that through at that time and were stopped. This time, we got them through and it is making a real difference and I am just really proud of you and the work that you are doing.

[The prepared statement of Ms. Buchanan appears as a submission for the record.]

Chairman HATCH. Now, let me just say I am proud of all of you and appreciate the work that each one of you is doing and the people that you work with, the staffs that you have and the organizations that you head. I am sure you are all aware that DOJ's Child Exploitation and Obscenity Section prosecuted only a handful of pure obscenity cases during the 8 years of the Clinton administration. During this same time period, there was a tremendous growth in the availability of pornography on the Internet. Will you please discuss how these challenges affected the Department's prosecution of obscenity cases right up until today. We will start with you, Mr. Malcolm.

Mr. MALCOLM. Certainly, Mr. Chairman. I think it is safe to say that there was a lack of Federal obscenity enforcement during the last administration, not on child porn issues, but on adult obscene material, and in part—

Chairman HATCH. I am not trying to pick on anybody. I am just citing what really are facts.

Mr. MALCOLM. Facts are difficult to ignore in this area, and the facts speak for themselves. I think that, coupled with emerging technology, certainly lead to a proliferation of obscene material. I mean, people who are going to be able to get a free pass and engage in illegal activity that is highly profitable are going to do so and do so in spades, and they did.

Unfortunately, also during that time period, we lost some very experienced prosecutors and investigators at the Federal level.

Chairman HATCH. I know the Department has faced significant personnel changes and challenges in this area, including an almost complete turnover of prosecutors at CEOS. Now that the new prosecutors are getting settled in and trained, should we expect to see

an increase in the number of investigations and prosecutions brought by the Department in this area?

Mr. MALCOLM. I absolutely do. We are coming up with an effective enforcement strategy, and it has taken us a while to get up and running, but now we are pretty much at a full clip and I fully expect—

Chairman HATCH. We expect you are going to full force forward.

Mr. MALCOLM. Absolutely.

Chairman HATCH. Okay. Mr. Flores, let me ask you this. As a member of the COPA Commission, you evaluated the accessibility, cost, and effectiveness of technologies to protect minors from sexually explicit material, harmful to minors material, which is different, on the Internet. Now, in your current position as Administrator of OJJDP, you hosted an Internet safety focus group that brought together experts in the government, private sector, and nonprofit organizations to discuss the increasing number of children and teenagers using the Internet, the proliferation of child pornography and the heightened activity by predators searching for unsupervised conduct with underaged victims.

Based on this experience, as well as your prosecutorial experience, what non-prosecutorial safeguards do you recommend to ensure that pornographic distributors cannot target children?

Mr. FLORES. Mr. Chairman, I think that question calls for two answers that are related. The first is that there are technologies out there, that when used carefully together, provide assistance to parents, to schools, to those locations where children have access to computer technology and the Internet. I don't think it is fair to say any longer that that technology is so nascent, that it is just not very good, it doesn't work, or it is very blunt and coarse in how it addresses these issues. So I think that, clearly, technology represents one of those tools that have to be used. I am glad to see that libraries and schools are now using these filters, they are putting them on their systems in order to provide a measure of protection.

But I would say that one of the things that came up at that focus group, and something that is extremely important to me, is the need and recognition that parents are still the missing cog in much of what we need to do to protect children. The Congress and the President have been very focused on the fact that industry has to take responsibility for what it does and what it makes available, whether it is the Internet service provider community or the direct purveyor and producer of the obscene material harmful to minors.

We have worked with schools and we have created educational materials and tools to teach kids safety. The National Center for Missing and Exploited Children does that. But one of the missing ingredients has been parents, and it has been a challenge to get parents engaged.

And so one of the things that the focus group has said is that if we want to succeed, we have got to find ways to encourage parents to really get involved. Because at the end of the day, the same thing is true that I told parents 15 years ago. If you want to protect your children from sexual abuse and predators, have a good relationship with them. Children who enjoy a solid and sound relationship with their parents have the least to fear and the smallest risk

of being exploited, whether it is through this technology or anything else.

Chairman HATCH. Let me just ask you, Ms. Buchanan, given your significant prosecutorial experience, will you explain to the Committee some of the unique challenges in prosecuting an obscenity case and how it compares with other, say, financial or violent crimes cases and how has the number and types of obscenity cases in your district been affected by Attorney General John Ashcroft's proclamation that obscenity prosecutions are a priority within the Department?

Ms. BUCHANAN. Every United States Attorney understood at the beginning of our terms that obscenity was a priority of President Bush and of Attorney General Ashcroft. I think that we all had to adjust our priorities in order to deal with the effects of terrorism, because that certainly is everyone's number one priority, and we do have to balance the current priorities of the Department, which include the prevention of terrorism, fighting corporate fraud, drug trafficking, and violent crime, and child exploitation and obscenity.

Some of the unique legal challenges I think that we will face in prosecuting these cases, first, members of the jury, I think are going to be very uncertain as to what the community standards are today because we haven't had prosecutions in this area really in the last decade. So much material has been made available to the public and I think that it has desensitized the public. People don't necessarily understand that the fact that certain things have not been prosecuted doesn't mean that they are not illegal.

The case that we are now prosecuting is really the first of its type in a decade, and this jury is going to have to decide what the community standard is. However, this particular case, wherever that line may be, it is so far over the line, we don't feel that it should be a difficulty in this case. But I think that finding and defining the community standard probably represents the greatest challenge in prosecuting obscenity cases.

Chairman HATCH. Thank you. Now, Mr. Maxwell, just a question or two for you before we finish with this panel. Your written testimony provides that over the last 6 years, the percentage of child exploitation cases investigated by the Postal Inspection Service that involve electronic communications increased from 33 to 70 percent. Now, how has this change in technology affected the way investigations are handled in the Postal Inspection Service?

Mr. MAXWELL. What we have found, there are a couple of challenges there that we have to face because of that. Sometimes the Internet solicitation and development of the case, which historically in years gone by would be through letter writing and mail, is much faster, number one.

Number two, there are a lot of nuances, obviously, in the investigative communications, but then also in setting up the actual—for Postal Inspectors especially, we normally like to have a mailing so we have a violation that we have jurisdiction over. We don't stop short, as I said earlier, we are with a task force and we are working it and the last minute, somebody may have experience with Postal Inspectors and says, I don't want to mail this. Let us meet and we will deliver it. We will still work that case, but that is a challenge we do face.

The other issues is that, you know, how widespread will it become. I agree with Mr. Flores as far as the prevention message to parents. There are countless things that they can do, and I think we need to do a better job maybe in getting that out. We did send out a—2 years ago, we had a prevention poster we put out which we had in each post office in the United States. It was designed by a young lady who was an artistic, graphic artist with computers and she wanted it to appeal not only to children, but to parents, and that was sort of the thought behind it. I think it was fairly well received.

That was—it took us forever to come up with that concept. We were so busy focusing on investigations, but what Bob had said earlier, I mean, there are ways that parents are knowledgeable, even if their children don't have dialogues with them often about what they personally do online, they can go to the histories and they can check things. So those all do present challenges.

Chairman HATCH. The Postal Inspection Service seems to have an advantage, or appears to have an advantage in investigating some obscenity and child pornography cases because the target usually will have purchased the material and have it shipped to their home, which thereby reveals the individual's name and address. Now, typically, how long does it take to conduct an investigation from its inception to arrest? How does it compare with other investigations conducted by other agencies?

Mr. MAXWELL. Not to give a lawyer answer and say it depends, but the true fact is it depends on the complexity of the investigation. Now, if it is a widespread type of operation, say in the case of Avalanche, where you walk into something that you realize is just tentacles to a lot of other things, it is going to take a lot longer. It depends on the complexity in tracing the assets. If there is going to be forfeiture or possibilities of capturing those assets, that could take a long time, so we could be talking months, and then possibly a year or two of litigation. If it is a quick hit with communications and a purchase, that is a lot easier.

So in short, to answer your question would be if it is a major operation, something to a greater extent, it is going to take longer because you have a much more complicated case to put together. If it is just a small-time operator or individual, things go right, it could be just a matter of months and less and then it could be pretty well wrapped up.

Chairman HATCH. Thank you. I appreciate all four of you and the work that you have done in the past, the work you are doing now, and the work that I believe you will be able to do even with more expedition in the future because of some of the tools that we have given to you and we intend to give more if you will help us to understand what would help you the most.

So in addition to your testimony today, if you will write to us and give us the rest of your ideas or any other ideas that you might have or you come across that might help us to correct prior legislation or improve upon legislation or enact prospective legislation, we would like to have your advice on it.

We appreciate each and every one of you. Thank you so much for being here.

Mr. MALCOLM. Thank you.

Mr. FLORES. Thank you, sir.

Mr. MAXWELL. Thank you.

Ms. BUCHANAN. Thank you.

Chairman HATCH. We will start with our panel two, which will consist of Mr. Bruce A. Taylor, President and Chief Counsel of the National Law Center for Children and Families in Fairfax, Virginia; Dr. Victor Cline, the Emeritus Professor at the University of Utah; and Mr. Steve Takeshita, the Officer in Charge of the Pornography Unit of the Organized Crime and Vice Division of the Los Angeles Police Department in Los Angeles, California.

It is good to see you, Dr. Cline. It has been a while since I have even said hello to you. It is great to have you here.

Mr. Taylor, we are going to start with you first, so we will take your statement, then we will take Dr. Cline's, and then we will take Mr. Takeshita's statement.

STATEMENT OF BRUCE A. TAYLOR, PRESIDENT AND CHIEF COUNSEL, NATIONAL LAW CENTER FOR CHILDREN AND FAMILIES, FAIRFAX, VIRGINIA

Mr. TAYLOR. Good afternoon, Mr. Chairman. As you know, I worked with you on bills going back to S. 1722 in 1977. I worked with your staff through the 1980's on the dial-up porn legislation, the child porn laws, and I think to this day that you were right in 1996 when you passed the Child Pornography Prevention Act to say computers are going to create images that look like real children, and if we can't find the kids, we may not be able to prove that it is real and we should deal with that kind of material as if it is child pornography.

But the Supreme Court last year said that Congress went too far. You can't criminalize computer images that aren't real. So Congress came back with the PROTECT Act, and you did several things, as you have been mentioning. One of the things was you took another tactic. We said, we will tighten up the definition so the Court can't extrapolate that maybe these laws could apply to Hollywood R-rated movies that they were never intended by Congress to apply to.

But you also gave law enforcement some new tools, like a new child porn obscenity law that says, if it is obscene and it portrays what appears to be children, we are going to increase the penalty. We are not going to let them get away with images just because we can't find the child. It is still child pornography to those pedophiles who think it is. It is still child pornography to those children who get seduced by it.

Real people get hurt by pornography. That is a message that we now focus on with child pornography. We now focus on it with some of the bondage and torture and rape and incest material that is floating around the Internet. But these are relatively new problems that as this Chairman and colleagues like Senator Grassley and others who have been on this Committee for the past 25 years have known have always been the fruits of the obscenity business.

I started prosecuting obscenity cases the day the Supreme Court announced the Miller decision in 1973. I did it in a small Bible-belt community called Cleveland, Ohio. I didn't have the luxury of starting off with animals and bondage and child porn. There was

no such thing. We prosecuted the adult porn syndicates for the adult pornography product that they brought into the American streams of commerce that Congress said was a felony, Ohio law said was a crime. New York law, California law, Texas law, and all the States have laws against obscenity. It has not been a failure of the American people that has led us to where we are today. It is more a failure of us in law enforcement.

Congress in the last eight or 10 years, as the Chairman noted, because there was no enforcement at Justice, and I was there from 1989 through 1994. We were allowed to continue the cases we had started, but there were not going to be any new obscenity cases. They didn't want to do them, so Congress said, well, we are going to pass better laws so that when we have prosecutors who will enforce Federal law, they will have better tools, and we did that. We passed the Communications Decency Act in 1996. In 1997, the Supreme Court said, well, the indecency standard is too vague, so Congress passed COPA in 1998.

Your statute that was passed in 1996 was replaced in 2003 with the PROTECT Act. The Communications Decency Act was reenacted in the PROTECT Act and now prohibits website operators and service providers from making obscenity and child porn available to minors. We have the law that makes libraries and schools use filters. Why? Because we are not only trying to protect kids from seeing adult pornography, but we are trying to encourage and give the tools to law enforcement to deal with illegal pornography.

It is my opinion as a prosecutor who has probably done more obscenity cases than anybody in the history of the country, in more communities across this country—I have done 100 trials in almost half of the United States—it is my opinion that we can still win because the people still consider obscene all hard-core pornography that shows penetration clearly visible. Our community standards did not sink into the sewer in the last 10 years so that only animals or bondage or children is going to be obscene to our juries. Like Mary Beth Buchanan, the U.S. Attorney from Pittsburgh said, our juries are going to have to be reeducated. They have forgotten that obscenity is a crime because there have not been any cases.

But one of the beauties of the Internet and the modern communication age is that a fewer number of cases will have a much greater impact on the crime than in the past. In the 1970's and 1980's, we had to get hundreds of convictions to make a dent in the pornography syndicates who controlled all the adult bookstores, all the theaters, all the video cassettes, all the TV, cable, radio. All of the pornography that was obscene in this country was tightly controlled by a couple of mafia families and a few major distributors.

They still run the show. There are more people involved in selling and distributing obscenity, but out of the 260 million webpages that have pornography on the web, there maybe are 150,000 websites. There are probably fewer than a few thousand web servers that host all those pictures. There are probably less than two dozen kingpins in the business who live in California and are controlled with associates in the mafia families in New York who control 90 percent of that.

A few well-placed prosecutions by the Federal Government and some of the bigger city district attorneys' offices will be able to

have the same deterrent effect on the obscenity business now that it has always had, meaning that when there are Federal prosecutions against child pornography, pedophiles are afraid to get it and they are afraid to molest children. When there are Federal obscenity cases, the pornography syndicates are afraid to distribute material.

They are deterred by the law when the law is used, and I think that our juries are still looking to us, meaning the Congress, to have better laws and law enforcement to enforce those laws, because we are going to set the standards that they will allow themselves and their children to learn from. We don't make the laws, we enforce them as prosecutors. But when Congress makes laws or State legislatures pass them and no one enforces them, the people think it must be legal or it wouldn't be there.

And that, I think, is the misconception that has been fostered on this generation. It is one that Congress has done what I think you have—you know, all you are able to do to make better laws. It is now up to a new administration, a new Attorney General. We have given him some time. There has been a lack of patience by a lot of groups that it has taken so long to get to where we are where they have started some cases. They had to hire new people. They had to train the people. But some things could still be done to make it better.

There needs to be more training. I think there should be more cooperation between State and Federal prosecutors, joint training of local prosecutors, cross-designating local district attorneys and county prosecutors to handle obscenity cases in Federal court. The lack of work power and manpower and resources in the Federal Government can be supported by having local prosecutors handle Federal cases. That is an established part of our system of cooperation and it can be done at very minimal cost.

It could also be the province of Congress to give the Postal Inspection Service ten or 20 new investigators to do obscenity and child porn, but obscenity in particular, maybe a couple of FBI agents to be assigned in headquarters to monitor and collect information about the organized crime networks and the pornography syndicates.

If obscenity cases are routinely done, the amount of fines and forfeitures far exceeds any budgetary expenditures of the law enforcement community. While I was at the Justice Department, in 5 years, the budget of the Department's CEOS, Child Exploitation and Obscenity Section, was $1 million a year and we took in $25 million in fines and forfeitures. It is not a reason that we enforce the law, but it is a very poor excuse to claim that prosecutors are using valuable resources to enforce these laws. The truth is that when the laws are enforced, the criminals pay for the cost of their own investigations and prosecution.

I think that that is what needs to be done and I would just like to make the record here today that all of the hard-core pornography that the syndicate imposes on the American public, whether it is through video cassettes, pay-per-view TV, or Internet, is still prosecutable in every one of our communities, in Utah as well as New York, in Dallas as well as Chicago. We can get convictions in all the big cities like we always have.

We need to encourage the Department not to be afraid but to go forward, and their young prosecutors will be more like I was when I started out and the chief prosecutor in Cleveland said to me, go do obscenity cases, and so for the next 3 years, I did 200 of them a year, not knowing that they were difficult and not knowing that people on the juries would have a second thought, because when they were given the chance to vote with their verdicts, they did. They told us what was obscene. We did not tell them. I think that is still the way it is. The American public are entitled to that presumption of their decency is still a community standard and that is why I would like to thank this Chairman and the members of the Committee for making this record that will encourage and, in a sense, require the Attorney General to keep going on the path he has started.

Chairman HATCH. Well, thank you, Bruce. We appreciate what you have done throughout all the years. You certainly have been a bulwark in this area and your advice and counsel has always been very helpful to us.

[The prepared statement of Mr. Taylor appears as a submission for the record.]

Chairman HATCH. Dr. Cline, we will turn to you now to take your testimony.

STATEMENT OF VICTOR CLINE, EMERITUS PROFESSOR, UNIVERSITY OF UTAH, SALT LAKE CITY, UTAH

Mr. CLINE. Thank you, Mr. Chairman. My name is Victor Cline. I am a clinical psychologist and psychotherapist specializing in marital and family counseling and the treatment of sexual compulsions and addictions. Also, I work with the victims of sexual abuse and assault. And additionally, I am a behavioral scientist with approximately 85 publications, many of which are in the area of media and pornography effects.

In the last 26 years, I have treated approximately 350 male sexual addicts or compulsives, including many pedophiles and their victims. I also treat rapists, voyeurs, fetishists, those making obscene phone calls, those compulsively promiscuous, et cetera, et cetera. These sexual illnesses all have a common core and dynamic base. They are sexual in nature, highly addictive, compulsive and repetitive, very difficult to treat, where self-control and self-discipline don't stop their occurrence.

The Internet represents, in my experience, an area of very significant risk for many children. Where parents have neglected to protect them with filters on their home computers or with frequent access to computers in public libraries, mots of which still lack protecting filters, this makes it exceedingly easy for children to peruse via the Internet explicit depictions of child-adult sex, rape, incest, bestiality, plus view cyber warehouses filled with other depictions of sexual aberrations. I see too many patients of minor age who are stimulated to practice or try out in real life the things they see in this material.

Now, the best evidence suggests to date that most or all sexual deviations are learned behaviors, usually through inadvertent or accidental conditioning. There is no convincing evidence to date suggesting the hereditary transmission of any pathological sexual

behavior pattern, such as pedophilia, rape, incest, exhibitionism, and so forth. In fact, one British psychologist, Dr. Stanley Rachman, demonstrated in the laboratory using live male subjects how easy it is to repeatedly condition normal males into sexual illness or addiction.

Child pornography is particularly pernicious because the child victims, whether they are sexually abused while being photographed or exposed to the erotic pictures as part of their seduction, are relatively powerless due to their young age and innocence and immaturity, as well as not fully understanding the harm potential. Their frequent willingness to trust an older person who appears to be kind and accepting of them makes them easy prey.

In my experience as a sexual therapist, any individual who regularly masturbates to pornography is at risk of becoming, in time, a sexual addict, as well as conditioning himself into having a sexual deviancy. In time, the high obtained from masturbating to pornography becomes more important than real-life relationships. It makes no difference if one is an eminent physician, attorney, minister, athlete, corporate executive, college president, unskilled laborer, President of the U.S., or an average 16-year-old boy. All can be self-conditioned into deviancy, and I have seen this for 25 years. I attend all the national meetings where these sorts of things and the research is discussed.

The process of masturbatory conditioning is inexorable and does not spontaneously remiss. The course of this illness may be slow and is nearly all hidden from view. It is usually a secret part of a man's life, and like a cancer, it keeps growing and spreading. It rarely ever reverses itself. It is also very difficult to treat and heal. Denial on the part of the addict and refusal to confront the problem are typical and predictable.

The presence of child pornography creates the potential of many types of harms in the community, including helping to create sexual predators or pedophiles and later their victims.

In the case of pedophiles, the overwhelming majority in my clinical experience use child pornography and/or create it to stimulate and whet their sexual appetites, which they masturbate to, then later use as a model for their own sexual acting out with children. I find that the use of child pornography in time desensitizes the viewer to its pathology, no matter how aberrant or disturbing. It becomes acceptable and preferred. The man always escalates to more deviant material and the acting out continues and escalates despite very painful consequences such as the destruction of the family, loss of spouse, children, job, health, or incarceration after committing criminal acts.

Some also use it to seduce children into engaging in sexual acts with themselves. When they introduce it to children, the suggestion is that this is normal behavior and many other young people like themselves also use it and do these things. I find that my pedophiles that I work with often trade, lend, and sell the pictures they make of young people nude and having sex through an informal network.

Some of the pornography they accumulate is of females fully developed anatomically, but made to look young and immature by dressing them in children's clothes and arranging their hair, such

as with a ponytail, to suggest to the viewer that they are underage minors when, in fact, they may not be. While the producers of this material may claim that no underage children were used in producing this pornographic material, to the viewer, this is irrelevant because they are perceived as minors by the psyche and this erotic arousal may generalize to all potential real child victims. Thank you.

Chairman HATCH. Thank you. That is startling testimony, but I know that you have worked long and hard in this particular area and have an international reputation and we are very appreciative for you taking the time to be with us.

[The prepared statement of Mr. Cline appears as a submission for the record.]

Chairman HATCH. Mr. Takeshita, we will take your testimony now.

STATEMENT OF STEVEN TAKESHITA, OFFICER IN CHARGE, PORNOGRAPHY UNIT, ORGANIZED CRIME AND VICE DIVISION, LOS ANGELES POLICE DEPARTMENT, LOS ANGELES, CALIFORNIA

Mr. TAKESHITA. Good afternoon, honorable Chairman and members of the Senate Judiciary Committee. I am Detective Steven Takeshita and I am the Officer in Charge of the Pornography Unit at the Organized Crime and Vice Division of the Los Angeles Police Department. Before I begin, I would like to thank the honorable Committee for your invitation to provide, which I hope will be useful testimony about the pornography industry.

I am a 25-year veteran of the department and I have been investigating the distribution of obscenity for the past 18 years. I have developed my expertise over the years by working with more experienced officers and by obtaining first-hand experience as an undercover operative in a joint investigation with the Federal Bureau of Investigation into the nationwide distribution of obscenity.

In the 1950s, the Los Angeles Police Department formed the Pornography Unit when it became aware that the pornography industry was developing its base in the Los Angeles area. The duties of the unit were to monitor the distribution of pornographic material and to prosecute the illegal distribution of obscenity as it affected the quality of life to the citizens of Los Angeles.

During this time period, the adult industry was taking advantage of the resources available in the Los Angeles area for their productions. The overabundance of unemployed hopeful adult actors and actresses and the support personnel who were willing to participate in the adult industry to meet their basic living expense and financial obligations. Because of the wide variety of scenic locations and the great weather, both the general and adult film industries favored the Los Angeles area. They could film a mountain, desert, or beach scene all in 1 day, an ideal environment for filming.

The industry has progressed from the "T.J. Bibles," sexually explicit pocketbooks bought in Tijuana, and eight-millimeter films to the DVD and the Internet. The Internet has been referred to as the "Wild West" of the 1990s. This Wild West of the 1990s has progressed to the point where the average distributor on the Internet

thinks that they are immune from prosecution because of the Internet. The Internet is just a vehicle for distribution. For example, if I were telephoning a minor to entice the minor for sexual activity, there would be no difference than if I chatted to that minor online for the same sexual activity. The Internet is just a vehicle the illegal activity.

This vehicle has posed new investigative methods. No longer do we respond to an advertisement in a local adult periodical to find the distributor in our backyard. Now, our response may be directed to a city across the nation or even a foreign country. Since our investigations deal directly with a person's First Amendment rights, all of our investigative evidence is acquired with either a search warrant or consent search. No longer can we establish agency liaisons only within our county, but now we must need to network with agencies across the nation and sometimes worldwide. These liaisons are critical for our surveillances and search warrants.

The Los Angeles area is no longer the base of distribution for 90 percent of the adult product within our Nation as it was in the earlier years. The increased use of the Internet has made the distribution of obscenity a national problem. The extreme adult product distributed nowadays was self-banned by the adult industry at large only 10 years ago. The recent hiatus in Federal prosecution of obscenity has brought forth the courage in the adult industry to produce this extreme sexually explicit product.

The adult industry must produce different types of products to encourage the consumer to continue in the purchasing of their product. The tight competition for the consumer dollar has encouraged the major adult industry producers to venture to the edge of the envelope with the distribution of some of the most extreme sexual product.

We have laws in place to protect the abuse the women endure during the filming of these extreme sexual videos. We have the laws in place to protect the exposure of this type of product to our children. We have the laws in place to create a better quality of life for our citizens. We need the assistance of the Federal Government to prosecute the violators of the statutes that Congress has enacted to put the welfare of our communities as one of our priorities.

Most recently, the Western District of Pennsylvania, Honorable United States Attorney Mary Beth Buchanan, who was here earlier, and her staff, the Child Exploitation and Obscenity Section, CEOS, of the United States Department of Justice, and the United States Postal Inspection Service have investigated and also assisted in our investigations in the distribution of obscenity. These entities have been very supportive and taken the lead into investigating the distribution of obscenity.

What we need today is for all law enforcement entities to prosecute aggressively any violator of the distribution of obscenity within their investigative jurisdiction to the maximum.

The First Amendment is listed first because our forefathers felt its importance. The adult industry tries to hide behind the First Amendment in the distribution of their product. The Supreme Court has ruled that the First Amendment does not protect obscenity.

I would like to thank the honorable Committee members for letting me have this opportunity to testify before you. Thank you.

Chairman HATCH. Thank you.

[The prepared statement of Mr. Takeshita appears as a submission for the record.]

Chairman HATCH. Thanks to each of you. We appreciate having you with us.

Let me start with you, Mr. Taylor. As I understand it, when you were at CEOS through the Child Exploitation Unit or Section and Obscenity Section in its early days, from 1989 to 1994, as you are probably aware, CEOS has had an almost complete turnover of its prosecutors in this administration. Can you please talk about some of the challenges that you faced when CEOS was in its inception and any observations as to how DOJ can meet the challenges it currently faces.

Mr. TAYLOR. In some ways, they are similar. One of the differences is that when CEOS was first created in the late 1980's, it tended to try to hire prosecutors who had some experience. So when I was brought in, we had a prosecutor from Oklahoma, Dallas, Buffalo, places where the prosecutors had already done obscenity cases and knew how to do it. We didn't have to learn the business, we just had to start the investigations. It still takes, as you found out today, three, six, 8 months to do an investigation, but we didn't have another lag time of a year or two to learn how to be the prosecutors.

The present staff of the CEOS is made up of a lot of bright young lawyers who did have to learn and are still learning the tricks of the trade of this business. The pornography lawyers know this business. They have been doing the same trials, the same arguments, same witnesses, same trial tactics and briefs for 30 years. There are some of us who have seen enough of their lawyers and their trials to know how to pass on to a new group of prosecutors sort of what they are going to see when they go to court, what the defense lawyer is going to say, what his witnesses are going to do.

But the good thing about the new prosecutors is that they are somewhat fearless. They do what they are told. You tell them to go to work, they do. They stay up late. They do their homework. Like I said, when I started out, I didn't know I couldn't do 200 obscenity cases a year. I didn't know we couldn't go after all of the people involved and we shouldn't be able to do every kind of material they do, and I think that could be the attitude that will save this CEOS group of lawyers from being discouraged or letting their guard down. I think they will go after the enforcement of the law as we expect Federal prosecutors to do, meaning spend all your time and all your effort doing as good a job as you can and you let the jury make the decision.

But we don't decide for the jury that they are not going to hear certain kinds of cases. We let them hear all of them, and I think we are more likely to see a bigger variety of cases out of this group over the next couple years, even though it has had to wait a couple of years because they had to start over and get trained. But I think we should start judging them starting today rather than from where they have come to.

Chairman HATCH. You feel pretty confident that this process is really in full swing now and that we are going to really start going after these people with—

Mr. TAYLOR. I do. I think that the Attorney General has meant it, since we met with him 2 years ago, that he wanted to enforce the law. It has been frustrating to say, well, they had to get a new chief, and they did. They had to get new lawyers, and they did. They had to train the lawyers, and they did. And so we have had to be patient while they had to start, and maybe the reason for the delay is that they hired people who didn't have the experience. That is up to them to decide how to do. It is not a criticism, but it is an explanation.

But now that they have had the time, they have got the staff, they know how to do it, I think that they will be able to do a good job and it will make a difference. It is not a losing proposition. There is no history of failure in Federal law enforcement in this area. There is always success among the juries when they are given a chance, and I think they will be given a lot of chances in the next 2 years.

Chairman HATCH. Thank you. Dr. Cline, in an article that you published in April of 1999, you indicate that about 94 percent of the 350 males that you treated for sexual addictions over the last 25 years, that pornography was a contributor, facilitator, or direct causal agent in acquiring these sexual illnesses. Moreover, you have stated that these illnesses are particularly difficult to treat, as you said earlier.

Do you think the greater proliferation of pornography now available on the Internet, on cable TV, and in hotels, do you think that this greater proliferation has contributed to the number of sexual addicts or hindered the treatment of sexual compulsions?

Mr. CLINE. I think that the ease in obtaining this material has actually facilitated the amount of pathology that we are seeing. In fact, Patrick Carnes, the world's leading researcher on this area has found that when he surveyed nearly 1,000 sexual addicts, he asked them the question of whether pornography had anything to do with it or not. Something like over 90 percent said, absolutely, the pornography is the thing that contributed ultimately to their criminal and their inappropriate or their sick kind of behavior, which now has become very addictive and repetitive and they can't control it.

Chairman HATCH. I have heard cases of very, very outstanding, religious, decent, honorable people who, once exposed to repetitive pornographic visualizations and obscenity, has had that exposure or exposures, have had those exposures just so distort their minds that they have a rough time handling it, many of them.

Mr. CLINE. Let me take a few—

Chairman HATCH. Have you had that experience?

Mr. CLINE. Yes. Oh, absolutely, again and again and again. I see corporate executives fired from their jobs because of sexual harassment and because they have gotten into this. They are using the computers that their company owns two or three hours a day, you know, into pornography and the company has a policy that that is not tolerated and they are losing their jobs and all kinds of consequences, especially for the man who is married. His wife reaches

a point where she can no longer tolerate it and the marriage is broken up. The husband promises he will quit, but he can't keep his promise.

Chairman HATCH. This could happen to anybody, any normal person who gets caught up in pornography?

Mr. CLINE. Especially males. The way we are wired, we are much more vulnerable than females, and most pornography is very hostile to women and very anti-feminine. There are major gender differences in who it is marketed to.

Chairman HATCH. And your testimony has been that with regard to children, it is even more volatile.

Mr. CLINE. Yes.

Chairman HATCH. Or difficult.

Mr. CLINE. See, there is a problem with the adults who are into it, so it goes far beyond just the child pornography. But if an adult masturbates to child porn and this gets them turned on and excited, then what this does is this creates within them over time an attraction toward children and eventually wanting to act it out and to have some kind of sexual contact with children. So both the adult and the child suffer.

Chairman HATCH. Mr. Takeshita, we are happy to have you, as well. Now, you mention in your written testimony that Los Angeles used to be responsible for the production of 90 percent of all pornographic material. The Internet has made distribution centers all over the nation. How much has this change in the Internet affected the portion of your investigations that are local versus multi-jurisdictional?

Mr. TAKESHITA. Our investigations generally have a basis in L.A. one way or the other. The product is either sent to the city or is distributed from the city. The Internet has made it so that the distribution point could be anywhere in the nation. The website owner or the person that owns the website may take our order and ship the product from his home to our jurisdiction.

Chairman HATCH. What sort of cooperation do you expect or do you receive from other law enforcement agencies?

Mr. TAKESHITA. The difficulty in our investigations is we have to show that the person we are going to prosecute, the owner of the business, has direct knowledge that his company is distributing sexually explicit product. That is one of the requirements for our prosecution.

With the cooperation of outside agencies, we would be able to have them do the fundamental surveillances, getting down as the location where the business is at, where his residence is at, so that when we go over and do our surveillances, we are not needed to be there for maybe a month to six weeks to establish a pattern. We can utilize the outside agency as our foothold into the investigation.

Chairman HATCH. Have you faced any challenges with an investigation you have worked on in California but then find it was prosecuted in another jurisdiction?

Mr. TAKESHITA. Usually, as you state, the investigation can be prosecuted either where the person is at or in California. Finding that type of conflict really doesn't occur. We usually have an open conversation with the investigative agency in the other State and

that is all settled before we ask them to assist us in our investigation.

Chairman HATCH. That is great. I will tell you, the testimony of you three has been very beneficial to us here today.

Again, I will challenge you to think in terms of how you might be able to help this Committee to come up with the changes in the law or improvement in the laws that currently exist that might help us to do a better job in this particular area. We hold these hearings to be able to try and come up with new and better ideas, and also to inform the public of the insidious nature of this type of activity. So please feel free to contact us and let us know how we can do a better job here in the United States Senate.

With that, this has been a very interesting hearing and one that we hope to act upon in the immediate future and we can use your help on it. So with that, we will recess until further notice. Thank you.

[Whereupon, at 3:37 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 8, 2004

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions posed by Senator Leahy to Ms. Mary Beth Buchanan, United States Attorney for the Western District of Pennsylvania, following Ms. Buchanan's appearance before the Committee on October 15, 2003. The subject of Ms. Buchanan's appearance was efforts of the Department of Justice to protect victims of pornography. We have also enclosed a corrected version of the transcript of Ms. Buchanan's testimony.

We hope you will find this information useful. Please do not hesitate to call upon us if we may be of additional assistance in connection with this or any other matter.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosures

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

93014.173

Response of Mary Beth Buchanan
To Questions Posed by Senator Leahy
Following October 15, 2003 Hearing on Indecent Exposure:
Oversight of DOJ's Efforts to Protect Pornography's Victims

1. **Peer-to-Peer networks allow individuals to share files with millions of other users in relative anonymity. Child pornographers now utilize these P2P networks to distribute the vilest forms of child pornography and are increasingly impervious to law enforcement scrutiny. Some P2P network operators take the position that the pornography reporting requirements do not apply to them.**

   a. **What are the unique challenges you face in prosecuting individuals that use P2P networks to distribute pornography?**

The challenges arise largely from the decentralized way in which P2P software generally operates to allow communication. P2P systems or "networks" are simply a group of individual computers sharing files with one another at any given point in time, which is facilitated by the use of P2P software. Because the computers generally communicate with one another directly, rather than through a central server, there are often no log records of file transactions between P2P users. Although P2P programs existed previously that did utilize a central server system (such as Napster), this type of P2P software is virtually non-existent now because of the potential liability attributable to the central server if individuals using the server are engaged in unlawful activity. There is also no incentive for those trading illegal files to return to the less anonymous central server system.

Further complicating matters is the fact that the computers of the individual users who utilize P2P typically provide scant evidence to support a prosecution. The P2P software on each individual's computer does not generate log records, and if it did, no one would have access to that content except the individual computer owner, who would also have the ability to disable the record-keeping function or delete records altogether in order to secrete illegal activity. Because an individual user's P2P software installed on his computer generally does not keep log records of file transactions, if an individual's computer is seized and found to house file-sharing software and a shared file containing child pornography, it often will be difficult to determine through computer forensics whether the user ever accessed the files in the shared file after receiving them, which impacts the ability to prove knowing receipt, possession, or distribution of child pornography.

Given the frequent absence of historical evidence in the form of log records, in order to most effectively investigate P2P cases, law enforcement must conduct undercover investigations in real time by identifying the internet protocol (IP) addresses of persons sharing illicit files at the moment the files are being exchanged. Law enforcement authorities must then use legal process to obtain the identity of the individuals associated with those IP addresses. This requires a proactive and time-intensive approach by law enforcement, and creates the need for substantial additional training in online undercover investigations and computer forensics.

93014.174

I have been told that P2P companies are promising that future generations of their software will provide users increased anonymity to shield users from detection and observation over the Internet by law enforcement and copyright holders. To make P2P users more anonymous, P2P software will use such techniques as encryption, port-hopping, proxy servers, and firewall-like features that screen out remote enquiries from watchdogs like law enforcement or copyright holders. While these tools may serve some legitimate purpose for those who use P2P networks responsibly, they will undoubtedly make those who abuse P2P networks harder to catch.

b. Would enforcing the pornography requirements against the P2P network operators improve your ability to prosecute these cases?

It is unclear what is meant by "pornography requirements" in this question. It could refer to the requirement that providers of electronic communication services and remote computing services report apparent violations of the Federal child pornography laws to the National Center for Missing and Exploited Children, as required by 42 U.S.C. § 13032. By contrast, "pornography requirements" could refer to the Federal child pornography laws themselves, which prohibit, *inter alia*, the knowing transport or distribution of child pornography, *see* 18 U.S.C. § 2252(a)(1), (2), and/or to Federal obscenity law, which prohibits the knowing transport of obscenity, *see* 18 U.S.C. § 1462.

If "pornography requirements" refers to the reporting requirements under 42 U.S.C. § 13032, it does not appear that we can enforce those requirements against "P2P network operators." As discussed above, the term "network" in the P2P context generally does not connote a central authority with oversight over file sharing transactions but, rather, simply means a series of individual computers sharing files with one another at any given moment. These individuals as a general matter do not constitute providers of electronic communication services or remote computing services - - the entities required to report under Section 13032.

In addition, it is unclear whether the distributors of the software that allows individuals to share files on their computers (such as KaZaA or Grokster) have any specific knowledge of, involvement in, or control over the exchange of specific child pornography files via P2P software. So far as we are aware, these software distributors do not provide electronic communications services or remote computing services, and therefore, also do not fall within the mandate of Section 13032. Moreover, even if P2P software were technologically capable of allowing its manufacturers to monitor the activities of their users, and even if the manufacturers qualified as providers of electronic communications services or remote computing services, 42 U.S.C. § 13032(e) specifically states that providers have no duty to monitor the content of their users' communications.

If "pornography requirements" in this question refers instead to the child pornography or obscenity laws themselves, the determination of whether the prohibition on transporting or distributing child pornography, or transporting obscenity, can be applied to "network operators"

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00253 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.175

depends on the meaning of that term. If "network operators" is meant to indicate the distributors of P2P software, it would again be difficult to prove that any of these software distributors have any specific knowledge of, involvement in, or control over the exchange of specific pornography files via P2P software. If "network operators" is instead intended to mean the individual users who share files using P2P software, they are most certainly subject to prosecution, albeit in light of the issues raised in response to question 1(a), above.

Despite the difficulties inherent in investigations into the trade of child pornography over P2P systems, we are committed to doing all that we can to apprehend and bring to justice those who use P2P systems for this nefarious purpose. Already, FBI agents have taken a proactive approach by initiating real-time undercover investigations and by completing intensive training courses for their agents on this type of online investigation. While the technological limitations that exist today, and that are likely to multiply as technology advances, preclude large numbers of prosecutions based on P2P trading, we expect even a small number of prosecutions to have a significant deterrent effect.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00254 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.176

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 8, 2004

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed are responses to questions posed to Mr. Robert J. Flores, Administrator of the Office of Juvenile Justice and Delinquency Prevention, following Mr. Flores' appearance before the Committee of October 15, 2003. The subject of Mr. Flores' appearance was oversight of the Department's efforts to protect the victims of pornography. In preparing these responses, we consulted with the Department's Criminal Division to the extent that the responses implicate prosecutorial concerns and policies.

We hope this information is useful to you. If we may of additional assistance, we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

RESPONSES TO QUESTIONS FOR THE RECORD
Robert J. Flores
Administrator, Office of Juvenile Justice and Delinquency Prevention
Office of Justice Programs

Committee on the Judiciary
United States Senate

October 15, 2003

Question 1: ***In your written testimony you state that, "it is imperative that we shepherd federal investigative and prosecution resources carefully so that where appropriate cases are developed, they can be referred for federal prosecution, keeping in mind that the protection of our citizens from the harms caused by obscenity and pornography must remain a state and local responsibility as well."***

a. ***Do you agree that a greater role for state and local law enforcement of child pornography cases could alleviate some of the strain on federal resources?***

Answer: The proliferation of child pornography has presented a challenge that we can successfully meet only if we work together – state, local, federal and even international law enforcement. Recognizing this, the Department of Justice strongly supported the change to 42 U.S.C. § 13032 in the PROTECT Act – that allows the National Center for Missing and Exploited Children (NCMEC) to refer tips of child pornography received through the Cybertipline to state and local law enforcement with greater ease – through the ICAC task forces. Increasingly, Federal law enforcement is teaming up with state and local law enforcement in national operations – referring individual targets to them for investigation and prosecution. The sad fact is that there are enough offenders to keep all levels of law enforcement busy.

b. ***What types of cases are more "appropriate" for federal prosecution?***

Answer: While it is appropriate for Federal prosecutors to be involved with the prosecution of child pornography and child sexual enticement cases at all levels, the Department has focused its efforts in a manner calculated to achieve maximum impact and deterrence. The Department's strategy involves a focus on offenses that are uniquely multi-jurisdictional; involve commercial sales, production, or large organized groups; or involve the use of sophisticated technology. Even then, where possible, Federal law enforcement agents are increasingly teaming up with their state and local counterparts.

93014.178

However, it is important to recognize that many states have limited laws regarding child pornography and cyber-enticement, and/or grossly inadequate penalties. Such factors should, and are, considered in selecting the appropriate venue for prosecution. Nearly every Internet case implicates multiple jurisdictions simply by virtue of how the Internet operates. At one end of the spectrum, the simple receipt of a child pornography case will involve evidence from the jurisdiction where the image originated, the jurisdiction in which it was received, and the jurisdiction where the server of the Internet service provider (ISP) or providers is located. Similarly, online enticement cases most often involve suspects who target minors in other jurisdictions and travel interstate to meet them. At the other end of the spectrum, commercial websites can easily implicate numerous districts in the course of the cumbersome investigations required to track the ultimate target. Similarly, the investigation of online groups frequently results in hundreds or thousands of leads sent to multiple jurisdictions throughout the United States and abroad. These types of nationwide investigations of targets based on common evidence can only be coordinated at the Federal level, even though state and local law enforcement agencies play an integral role in ultimately apprehending suspects. In sum, the ability of Federal law enforcement to span all jurisdictions makes all types of Internet cases particularly suited for Federal involvement. However, Federal law enforcement increasingly recognizes the value of teaming with state and local law enforcement, and nearly all national investigations involve state and local resources, as well.

Finally, as Deputy Assistant Attorney General John Malcolm noted in his testimony, obscenity cases where the targets are significant producers, distributors, and facilitators of obscenity, and whose illegal products are widely marketed across jurisdictional lines, are uniquely appropriate federal targets. However, here too there is a significant, and perhaps even greater, role for state and local law enforcement, who will have the unique ability to assess the standards of their community, as required by the Supreme Court in obscenity prosecutions.

c. Are there particular cases that would be best handled by local and state law enforcement?

Answer: As noted above, because of the unique multi-jurisdictional implications of these Internet-based offenses, this category of case is nearly universally suited for federal prosecution. However, as also noted above, Federal law enforcement usually teams up with state and local law enforcement – with

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00257 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.179

the latter handling many of the leads or targets in their respective jurisdictions that are identified by the larger operation. In sum, there is no evident or logical split for these cases. However, we are fortunate that, in this area, there exists close cooperation between law enforcement agencies, including with state and local law enforcement agencies. Together, they have been making a difference, and we are confident that this partnering will continue to yield results.

d. ***Do you have specific suggestions for how federal investigative and prosecution resources can be used more carefully?***

Answer: Yes. I firmly believe that, in addition to their continued cooperative approach, local, state and Federal law enforcement authorities must receive appropriate, consistent, and compatible training. This is a highly technical field that requires the highest standards of investigation and prosecution to allow all levels of law enforcement to prosecute these cases efficiently and effectively. This training is necessary for both investigators and prosecutors, who often face well-financed and extremely experienced defense counsel.

I also believe that it is important to ensure that resources are not being duplicated. The Department last year put in place a notification system to ensure that all districts be notified of an operation with nationwide impact at its earliest stages. This system is one further step in our ongoing attempts to strengthen cooperation and information-sharing in this critical area.

Question 2: ***The Victims of Child Abuse Act, as amended, requires electronic communication services or remote computing services to report incidents of child pornography to the National Center for Missing and Exploited Children (NCMEC) and authorizes NCMEC to forward these reports to a law enforcement agency or agencies designated by the Attorney General. In your submission, you mention that these reports are available online in "real time" to the Federal Bureau of Investigation (FBI), the Bureau of Immigration and Customs Enforcement (ICE), and the Internet Crimes Against Children (ICAC) Task Forces.***

a. ***Do you believe other law enforcement groups should have "real time" access to these reports? If so, please identify those groups.***

Answer: Since my testimony, the Attorney General designated the United States Postal Inspection Service and the United States Secret Service as additional recipients of the reports, or tips. *See* 28 C.F.R. § 81.13.

In responding to this question, it is important to consider the potential ramification of opening the Cybertipline reports for broad dissemination to

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00258 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.180

law enforcement agencies across the country. The unfortunate reality is the vast majority of law enforcement agencies in the United States do not have the investigative expertise or technical capacity to follow up on a Cybertipline report. By providing this information to an unprepared and ill-equipped law enforcement agency, we run the risk of that report not being effectively worked or, worse yet, not worked at all. By keeping the Cybertipline reports limited to select agencies, we ensure more effective investigations, either directly through, or at the guidance of, trained law enforcement. With the addition of ICAC task forces as recipients of the reports, many local law enforcement agencies now have effective access to the cases as they work together with Federal partners. This important tool assists in building further partnerships in a controlled setting.

b. Peer-to-Peer networks have been shown to harbor vile forms of pornography. Are you aware of efforts to require peer-to-peer network operators to report incidents of pornography pursuant to the Victims of Child Abuse Act, as amended?

Answer: Unlike the original peer-to-peer (P2P) networks, such as the early versions of Napster and Morpheus, which operated from a central server or series of servers, the current conventional P2P applications are all software-based. In other words, there is no central network that can monitor the distribution of any file between users.

The simplest explanation of how this software works is that it allows a user to select from a list of products (downloads) with limited descriptions available from a volunteer computer (Super Node). That Super Node, of which there are thousands, if not tens of thousands, then gives the requesting computer a digital address (IP Address) of the computer or computers that hold the complete file that is of interest. Once the Super Node delivers the IP address to the requesting computer, a direct, but brief, link is established between the requesting computer and the computer with the file of interest. The Super Node does not retain any files pertaining to the download. With that information in mind, the P2P software companies, such as Kazaa, Napster, and Morpheus do not monitor networks. They develop and sell software with product applications for the end users.

In short, it appears that the operating environment created by the current P2P networks does not provide for monitoring the fleeting connection between users in order to report to NCMEC the incidents of pornography pursuant to the Victims of Child Abuse Act, as amended.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00259 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.181

c. ***Do you agree that it would improve enforcement against child pornography if the peer-to-peer network operators complied with these reporting requirements?***

Answer: As described previously, it is my understanding that the operating environment of the software does not provide monitoring applications. Unless there are P2P networks still operating from a traditional server system, they have no knowledge of which files are being transferred to which users, and therefore have no basis to report. If peer-to-peer providers came within the ambit of the reporting statute (which they currently do not) and if they monitored the systems or otherwise captured log data (which they generally do not, and are not required to do), then reporting would be helpful.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00260 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.182

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 8, 2004

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions posed by Senator Leahy to Deputy Assistant Attorney General John G. Malcolm of the Department's Criminal Division following Mr. Malcolm's appearance before the Committee on October 15, 2003. The subject of the hearing was the Department's efforts to protect victims of pornography.

We hope that this information is helpful to you. If we may be of additional assistance we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

Enclosure

93014.183

RESPONSES TO QUESTIONS POSED BY SENATOR LEAHY FOLLOWING THE HEARING ON INDECENT EXPOSURE: OVERSIGHT OF DOJ' EFFORTS TO PROTECT PORNOGRAPHY'S VICTIMS

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

OCTOBER 15, 2003

1. **In your written testimony, you state that "[w]hile the Department is committed to a renewed enforcement agenda with regard to adult obscenity, and despite the obvious divergence of federal resources to combat terrorism, the Department continues to vigorously enforce child sexual exploitation laws."**

   a. **What is the composition of the child pornography cases that the Department currently handles? Please provide the percentage of cases that are sexual exploitation cases under 18 U.S.C. Section 2251 (including so-called traveler cases prohibiting the enticement of minors interstate for the purpose of engaging in sexually explicit conduct), cases that involve the sale, receipt or transport of child pornography under 18 U.S.C. Sections 2252(a)(1), (a)(2), (3) or (4), and cases that involve only the knowing possession of child pornography under 18 U.S.C. Sections 2252(a)(4) or 2252(a)(5). Please also indicate whether there have been any prosecutions under Section 2251A involving the selling or buying of children? If so, please describe.**

All of the cases that fall under 18 U.S.C. § 2251, which criminalizes the production of child pornography and the advertisement of child pornography, involve sexual exploitation. The "traveler" cases that you refer to are generally governed by Title 18, Sections 2421 (Transportation generally), 2422 (Coercion and enticement), and 2423 (Transportation of minors). We are unable to provide the percentages of cases under particular subsections of Sections 2252 because the case statistics are not kept by subsection or by statute, but rather by groups of statutes. Statistics available to us indicate that in 2002, there were 1,119 cases filed involving child pornography, "travelers," and/or sexual abuse (under Chapter 110, 18 U.S.C. Sections 2251-2260, and/or 18 U.S.C. Sections 2241, 2243 and 2423), resulting in 868 convictions. Of those cases filed, 764 involved child pornography exclusively, resulting in 585 convictions.

   b. **Do you agree that a greater role for state and local law enforcement of child child pornography cases could alleviate some of the strain on Department resources?**

The enforcement of child exploitation crimes is one area where we cannot afford to fail. Yet the Internet's ease of access and distribution present significant challenges to law

93014.184

enforcement because child pornographers can trade images with relative ease and child predators have ready access to innocent children. As a result, we need to bring every resource we have to bear on the problem – federal, state, local and even international. It is for this reason that the Department strongly favored the change to 42 U.S.C. § 13032 allowing the National Center for Missing and Exploited Children (NCMEC) to refer tips from the Cybertipline directly to state and local authorities, including the Internet Crimes Against Children (ICAC) Task Forces. More than ever before, the Department is partnering closely with NCMEC and the ICAC Task Forces to ensure that all our resources are used, in a coordinated fashion, to tackle this vexing problem.

c. Do you agree that a significant portion of the child pornography cases handled by the Department could also be handled by state and local law enforcement?

I do not agree with that suggestion. While state and local law enforcement are equipped to handle, and should handle, the investigation and prosecution of many child pornography offenses, the multi-jurisdictional nature of today's cases makes it impossible for any single jurisdiction to handle the large Internet-based cases that identify pornographers and predators throughout the United States and the world. For example, many of the child pornography cases that are handled federally arise from "national operations." The Internet is replete with "chat rooms," "groups," "bulletin boards" and other relatively secure cyber meeting places. Pornographers form these groups and gather in these groups in great numbers. On any given day, the High Tech Investigative Unit of the Department's Child Exploitation and Obscenity Section (CEOS) can identify in a matter of minutes a handful of new groups dedicated to the exchange of child pornography. There are probably hundreds of these groups operating at any given time. Each group can easily boast thousands of members, strewn throughout the United States and the world. Additionally, commercial websites that provide child pornography can also be found on the Internet with relative ease. The investigations of these groups, websites, and website customers require technical skill and speed (because ISPs do not typically retain records for long periods of time) to preliminarily identify the thousands of offenders. Then, all the relevant information on the group(s), websites, and the offenders must be obtained from various ISPs, packaged and quickly referred for target-specific investigation to establish probable cause on the subject. Speed is of the essence because of staleness issues.

CEOS, which I oversee, has taken an active role leading the Department and our federal partners (Bureau of Immigration and Customs Enforcement (ICE), U.S. Postal Inspection Service, etc.) to target the uniquely federal offenders (commercial websites, nationwide groups, etc.) and to parse out customer-specific investigations to state and local authorities where possible. Indeed, the FBI's current practice is to work closely with ICACs at the very onset of a national operation to ensure that customer-specific investigations are properly funneled to state and local authorities. As an example, the FBI has developed a national initiative targeting the trade of child pornography on peer-to-peer networks. The FBI and CEOS have already scheduled a meeting with the ICACs, before the initiative is implemented, to coordinate their respective roles.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00263 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.185

In short, the Department fully appreciates the importance of using limited Federal resources in a way that guarantees the most impact (i.e., the technically difficult or complex cases, and nationwide or international operations). The Department also firmly believes that to be effective, we must partner solidly with other Federal agencies and state and local authorities. Together, in a coordinated fashion, we can make the biggest impact.

d. Section 9-75.420 of the U.S. Attorney's Manual states that "Federal prosecution of obscenity and child pornography cases should focus upon producers and interstate distributors. However, cases involving straight possession may warrant federal prosecution and production and distribution cases may be more appropriately prosecuted in state court. Moreover, many cases include both federal charges (such as distribution of pornography) and local charges (such as sexual abuse). Hence, cooperation between federal and local officers and prosecutors is strongly encouraged and can be highly productive in both federal and local efforts. See Fed.R.Cr.P. 6(e). The formation of multi-agency and multi-jurisdictional task forces is strongly encouraged" (1) How does this policy statement comport with Section 9-75.020's instruction that all prosecution of all child pornography cases are "highly encouraged." (2) Are there uniform guidelines within the Department of Justice regarding when a particular child pornography possession case should be prosecuted federally or by local authorities? What about receipt or transport cases? Cases involving minors who are enticed to travel to engage in sexually explicit conduct? If there are such internal guidelines, please provide a copy. (3) Can you describe all multi-agency and multi-jurisdictional task forces currently in existence?

(1) The United States Attorney's Manual (USAM) policy statements identified in the question are complementary. The goal is to impart the importance placed on child exploitation cases but to also recognize the reality that some (or even most) U.S. Attorneys' Offices do not have the resources to prosecute all child exploitation cases referred to them for prosecution. In that event, the USAM parses out the factors that tend to make one child exploitation offense more serious, or more befitting Federal prosecution than another.

The sad fact is that Federal agents and prosecutors cannot pursue all child exploitation offenses. The number of offenders is simply overwhelming. The Department's goal, described in more detail above, is to organize the enforcement efforts of state, local and Federal authorities to ensure we all work within a common plan of attack. If we succeed in this endeavor (and certainly we are far better off today than we were even one year ago), only appropriately federal cases will be referred to U.S. Attorneys' Offices for prosecution and, in principle, no cases should be declined in favor of state prosecution. In other words, the goal is to resolve these important issues on the front end, rather than leaving it to chance at the tail end.

(2) See response to (1), above.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00264 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.186

(3) There are numerous multi-agency, multi-jurisdictional task forces currently in existence. Foremost among them are the 45 Office of Juvenile Justice and Delinquency Prevention (OJJDP) funded ICAC Task Forces. While these units do not have a standard agency composition requirement, the majority do include law enforcement and prosecutorial representatives from multiple local, state and Federal agencies. In at least three examples, the ICAC Task Force is co-located and/or task force members are assigned directly with the FBI's Innocent Images units, to include the Safe Team in Los Angeles, California, and units in Salt Lake City, Utah, and Cleveland, Ohio.

Due to the ever increasing need for general computer forensic and investigative expertise, the ICAC Task Forces and law enforcement in general, are joining regional computer crime centers that include FBI, DHS ICE, the Secret Service, and the US Postal Inspectors. Specific examples of these centers include the Sacramento Valley High Tech Crime Center; the St. Louis, Missouri, Regional Computer Crime Education and Enforcement Group; and the South Carolina Computer Crimes Center.

In addition, the Department has recently undertaken a child prostitution enforcement initiative dubbed "Innocence Lost." The initiative targets 13 districts identified as having a high incidence of child prostitution. The initiative rests upon a multi-disciplinary, task force approach. To establish an effective integrated approach, essential to the successful prosecution of these cases, the program brings together state and federal law enforcement agencies, prosecutors, and social service providers to facilitate cooperation and partnership among them. In "Innocence Lost," the FBI and CEOS have partnered with NCMEC. Together, we have developed an intensive week-long training seminar solely dedicated to the investigation and prosecution of cases involving child prostitution. The pilot training program occurred during the week of September 15, 2003, and the most recent seminar began on February 29, 2004. Participants were drawn from the 13 districts initially identified by the FBI as having a high incidence of child prostitution. There will be at least two additional training programs in 2004 specifically addressing child prostitution and covering various regions of the country (the next conference is scheduled for July 11, 2004).

Another important example of a task force or cooperative approach involves the National Crime Victim Identification Program (NCVIP). The NCVIP is a cooperative effort between Federal partners (ICE, FBI, U.S. Postal Inspection Service) and state and locals (through NCMEC), whereby Federal and state investigators work together to identify child pornographic images depicting fresh abuse, to identify and rescue the child, and identify and punish the offender.

Finally, there are a number of other examples of state/Federal cooperative approaches to the issue. A good example is the SAFE Team in Los Angeles, CA. The SAFE Team is comprised of state and local law enforcement, FBI, and ICE. Members of the team work together to investigate and prosecute child exploitation cases.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00265 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.187

2. **The Victims of Child Abuse Act, as amended, requires electronic communication services and remote computing services to report incidents of child pornography. What is the status of the Department's implementing regulations to provide guidance to Internet Service Providers reporting under the Victims of Abuse Act, pursuant to the PROTECT Act?**

The Attorney General is authorized to designate the law enforcement agencies to which reports may be forwarded by the National Center for Missing and Exploited Children ("NCMEC"), but the statute does not authorize implementing regulations to impose duties on internet service providers ("ISPs"). *See* 42 U.S.C. § 13032(b)(2). Accordingly, the regulations can suggest, but not require, that ISPs report suspected violations in specific ways. The vast majority of large ISPs with whom the Department has consulted have indicated a desire to implement reporting in the manner most useful to NCMEC and the law enforcement community. The Department has been working with NCMEC, the Federal Bureau of Investigation, the Department of Homeland Security's Bureau of Immigration and Customs Enforcement the United States Secret Service, the United States Postal Inspection Service, and the major ISPs to achieve consensus on the reporting protocols. This is a time-consuming process, particularly because of the technical constraints of both the individual ISPs and NCMEC that necessarily dictate the limits of any reporting protocol. The Attorney General published the initial designation of four law enforcement agencies to which NCMEC should forward reports on November 4, 2003. *See* 28 C.F.R. 81.11 *et seq.* As the Department gathers a consensus on a more comprehensive set of guidelines both for IPSs reporting to NCMEC and for NCMEC's reports to law enforcement, the Department will publish these operating guidelines. The Department appreciates the support of the ISPs in this endeavor and expects to be able to develop a consensus protocol.

3. **Peer-to-Peer networks allow individuals to share files with millions of other users in relative anonymity. Child pornographers now utilize the P2P networks to distribute the vilest forms of child pornography and are increasingly impervious to law enforcement scrutiny. Some P2P network operators take the position that the pornography reporting requirements do not apply to them.**

   a. **What is the Department's position on whether the pornography reporting requirements apply to these P2P networks? If the Department has not concluded that these requirements are applicable to P2P networks, please explain why not.**

The term "network" in the P2P context generally does not connote a central authority with oversight over file sharing transactions, but rather, simply means a series of individual computers sharing files with one another at any given moment. As a result, it is unclear whether the distributors of the software that allows individuals to share files on their computers (such as KaZaA) have any specific knowledge of, involvement in, or control over this activity. So far as I am aware, these software distributors do not provide "electronic communications services" or

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00266 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.188

"remote computing services" as those terms are statutorily defined, *see* 18 U.S.C. §§ 2510(15), 2711(2), and, therefore, do not fall within the mandate of 42 U.S.C. § 13032. Moreover, even if P2P software were technologically capable of allowing its manufacturers to monitor the activities of their users, and even if the manufacturers qualified as providers of electronic communications services or remote computing services, 42 U.S.C. § 13032(e) specifically states that providers have no duty to monitor the content of their users' communications.

In that the "networks" in the P2P context generally consist of ordinary citizens trading files, those individuals also do not fall within the mandatory reporting statute. Nevertheless, citizens do report the presence of child pornography on the Internet to the National Center for Missing and Exploited Children's Cyber Tipline, though this is purely voluntary.

b. What is the Department's progress in pursuing child pornographers that use P2P networks as a means of distributing child pornography?

In addition to the substantial volume of child pornography available on P2P networks, the Department believes that this scourge may be even more prevalent in other Internet fora, such as commercial websites, newsgroups, and Internet Relay Chatrooms (more commonly referred to as IRCs). Nonetheless, the Department recognizes that child pornography is proliferating on P2P networks and we are focused on addressing this problem. In that regard, the FBI has trained approximately 30 special agents from FBI field offices around the country on P2P technology and the FBI protocol for investigating P2P networks. This training will form the basis of the FBI's larger plan to decrease the proliferation of child pornography on P2P networks. The FBI is also currently providing investigative support on numerous P2P cases that are in various stages of investigation or prosecution throughout the Nation.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00267 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.189

Questions for Bruce A. Taylor, President & Chief Counsel
National Law Center for Children and Families

1. Peer-to-Peer networks allow individuals to share files with millions of other users in relative anonymity. Child pornographers now utilize these P2P networks to distribute the vilest forms of child pornography and are increasingly impervious to law enforcement scrutiny. Some P2P network operators take the position that the pornography reporting requirements do not apply to them.

    a. Are you aware of efforts to require peer-to-peer network operators to report incidents of pornography to the National Center National Center for Missing and Exploited Children pursuant to the Victims of Child Abuse Act, as amended?

    b. Do you agree that it would improve enforcement against child pornography if the peer-to-peer network operators complied with these reporting requirements?

93014.269

SUBMISSIONS FOR THE RECORD

Department of Justice

STATEMENT

OF

MARY BETH BUCHANAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF PENNSYLVANIA

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

INDECENT EXPOSURE: EFFORTS OF THE DEPARTMENT OF JUSTICE TO PROTECT VICTIMS OF PORNOGRAPHY

PRESENTED ON

OCTOBER 15, 2003

93014.190

Testimony of Mary Beth Buchanan
United States Attorney
for the Western District of Pennsylvania

before the
Committee on the Judiciary
United States Senate

Indecent Exposure: Efforts of the Department of Justice to Protect Victims of Pornography

October 15, 2003

Mr. Chairman, Ranking Member Leahy, and esteemed Members of the Committee:

My name is Mary Beth Buchanan, and I am the United States Attorney for the Western District of Pennsylvania. I also serve as the Chairman of the Attorney General's Advisory Committee of United States Attorneys. It is an honor to appear before you to discuss the work of my office and of the United States Attorneys across the country to protect victims of pornography. Before my appointment as United States Attorney, I served as an Assistant United States Attorney in Pittsburgh for thirteen years. My work focused on cases involving the sexual exploitation of children. In that capacity, I prosecuted many predators who had a sexual interest in children. During the course of my work, I saw the nature of the cases in this area change dramatically. Initially, cases involved individuals trying to obtain child pornography by mail, usually in an unsophisticated manner. The activity of the perpetrators evolved during the 1990s, to include cases targeting adults who used the internet, not only to exchange child pornography, but to contact children and attempt to arrange meetings where sexual molestation would occur.

With respect to obscenity cases, much has changed, as well. The adult bookstore has largely been replaced by thousands of web sites advertising and selling pornography. Nearly everyone has received unwanted and offensive spam emails advertising graphic sexual material. Pornographic web sites also offer videotapes, "streaming video" and live web-cam activity, all of

93014.191

which can be accessed immediately by the computer user. Effectively, this means that the world's worst adult bookstore now operates on a personal computer in almost every home in America. It is not a leap of logic to assume that young people are accessing this material.

Thus, the work of the Department of Justice to provide a safe America for children now extends well beyond the physical world into the electronic universe of cyberspace. The Internet offers unparalleled educational opportunities for our children. But there are dark corners of the internet where children are being exposed to inappropriate sexual material and where they may be susceptible to predators who view them as sexual objects. Protecting children is the most important reason to vigorously enforce both our federal child exploitation laws and our laws against distributing obscenity.

Let me tell you about some cases we have prosecuted in the Western District of Pennsylvania that demonstrate how the Internet can be misused.

Several years ago, I prosecuted an Arizona minister who had befriended a 13 year old boy on the internet. He sent the boy child pornography. He also sent the boy a camera and encouraged him to take sexually explicit photographs of himself and then mail them to the minister. Fortunately, the boy's parents discovered the pornography on their son's computer and contacted the FBI. A search of the minister's residence revealed hundreds of photographs, computer discs and magazines containing child pornography. The minister received a ten-year sentence and the information seized from his residence led to child pornography prosecutions in other districts throughout the country.

Another case began with a lead from the search of a child pornographer's residence in Harrisburg. The Harrisburg man had been trading child pornography with a man from Western

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00271 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.192

Pennsylvania. A search warrant executed in our district revealed numerous boxes of child pornography and adult pornography located within the residence. Most importantly, the agents found a videotape made when the perpetrator filmed himself having sex with his drugged and asleep 11 year old niece. He had taken his niece to an amusement park in Ohio as a "birthday present" and molested her without her knowledge. The judge imposed a 15-1/2 year sentence upon conviction.

In a similar case which occurred just this year, the FBI received information that a Pittsburgh man had been attempting to trade child pornography with an undercover detective in Chicago. A search warrant for child pornography was executed at his residence. Located at the scene when the agents arrived was a ten-year old girl whom he had adopted in Russia for the primary purpose of sexually abusing her. Fortunately, the girl revealed the abuse to an FBI agent participating in the search. The defendant recently pleaded guilty and is facing a sentence of 15 to 20 years in prison.

In another case, a defendant convicted of possession of child pornography in Los Angeles agreed to cooperate with investigators in Pittsburgh. The Los Angeles defendant revealed that he had been watching a Pittsburgh man have sex with his five-year old daughter live over the Internet. The Pittsburgh man had even sold pairs of his daughter's underpants to the cooperator. Images of the molestation were captured, and the Pittsburgh man, who had a previous conviction for possession of child pornography, was sentenced to nine years in prison. These events occurred in a 1997 case. The defendant would be facing a mandatory minimum 25 year prison term under the PROTECT Act today.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00272 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.193

All of these individuals possessed thousands of images of child pornography, revealing their strong interest in sex with children. Unfortunately, these perpetrators did not stop with the mere viewing of images - they acted upon their perverse sexual interests.

As the extensive nature of the child pornography collections we see reveals, perpetrators are collecting more material, and the internet makes it easy. They are creating a market which demands more and newer images. This, of course, means that more children will be molested. Every collection of thousands of images shows the terrible abuse of real children. These real children are re-exploited each time their image is transmitted to a new person.

More recently, we prosecuted a man from Virginia who identified himself on the Internet as a "Master of Teen Slave Girls." He engaged in chat conversations over the Internet with a thirteen year old girl from Pittsburgh for several months. On New Year's Day of 2002 he transported her to his house in Virginia where he sexually assaulted her. He also created a video as he abused her and transmitted it over the internet to a man in another state. The defendant pleaded guilty to producing child pornography and received a twenty year sentence. Once again, his computer contained thousands of images of adult and child pornography. It was clear from reviewing the material on his computer that pornography had fueled his desire for sex with children, and that the Internet had provided him with the opportunity.

In these cases, and many others, we have found a direct link between adult and child pornography and offenders who actually molest children. Images now available on the Internet are more graphic, involve younger children being molested, and increase every day.

There are few, if any, crimes more serious than the rape of a child. United States Attorneys have placed a high priority upon catching and prosecuting these offenders, and we

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00273 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.194

work closely with the Child Exploitation and Obscenity Section (CEOS) of the Department of Justice on these cases. We also recognize the importance of coordinating our efforts with state and local authorities.

The importance of cooperation among law enforcement professionals, as well as the integration of agencies serving victims and medical professionals, led to the formation in my district of the Western Pennsylvania Crimes Against Children Task Force. The Task Force was initially funded by the Office for Victims of Crime within the Department of Justice. Our task force includes federal and state prosecutors, the Federal Bureau of Investigation, the United States Postal Inspection Service, and other federal law enforcement agencies, officers from the sex crimes units of the state, county and city police, medical professionals, including forensic examiners, from two major Pittsburgh hospitals, representatives from social service agencies which assist victims of crime, and attorneys from Kids Voice, a local agency which represents dependent children in court. By combining these resources and exchanging information frequently, we are able to ensure that the unique needs of child victims are met. The needs of the child are given our first priority. Coordination among all reduces the number of times that a child must be interviewed and ensures that the strongest case and longest sentence is pursued.

Let me now turn to the area of adult obscenity, as it is important to recognize that adults, as well as children, are often victims of pornography. With a CEOS trial attorney as a member of our prosecution team, we recently brought an indictment against Extreme Associates and its owners, Robert Zicari and Janet Romano. Extreme Associates, a California company, has produced some of the most vile, offensive, and degrading material available on the Internet. One of the videos charged as being obscene, Forced Entry, portrays the brutal rape and killings of

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00274 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.195

three women. The women are hit, slapped, and spit upon. Another video involves sexual acts with multiple men followed by the woman being made to drink almost every type of liquid excreted by humans. Although the third video apparently involves actresses of at least 18 years of age, it portrays sex with children. In one scene, a girl playing in a tent in her living room is shown having forced sex with a magazine salesman.

Obscenity, by its very nature, reduces human beings to sexual objects. Just last week I received a letter from a woman whose daughter had participated in the production of pornographic films. This mother described how her daughter, who had graduated from a high-ranking high school with an excellent record, had fallen into the world of pornography. The daughter has now been reduced to an anorexic drug addict with severely compromised mental and physical health. This mother, with no where else to look for help, has asked my office to continue to work to, and I am quoting from the letter, "prevent the exploitation and destruction of other young women."

My office, along with other United States Attorneys across the country, looks forward to continuing the fight against child pornography and obscenity. I thank you again for inviting me to speak before this Committee and would welcome any questions.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00275 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.196

U.S. Department of Justice

Washington, D.C. 20530

April 8, 2004

Honorable Orrin G. Hatch
Chairman
United States Senate
Committee on the Judiciary
Washington, DC 20510

Dear Chairman Hatch:

Thank you very much for inviting me to participate in the Judiciary Committee's October 15, 2003, hearing entitled "Indecent Exposure: Oversight of DOJ's Efforts to Protect Pornography's Victims." I appreciated the opportunity to discuss with the Committee, the efforts made by my office and the Department of Justice to fight pornography and to protect the American people.

I respectfully request the Committee's leave to make a substantive change to one portion of my testimony. In response to a question about the use of pen registers and trap-and-trace devices to track e-mail and Internet use, I stated that such tools were very useful in a non-terrorism case involving a Virginia man who lured a 13-year old girl from her home and sexually abused her. I made this statement based on information that had been provided to me.

I have since learned that information was inaccurate, and apologize for the inaccuracy of my statement at the hearing. The agents and prosecutors investigating Scott Tyree, the Virginia man, used Section 212 (which allows providers of electronic communications to disclose communications in life-threatening emergencies) and Section 220 (which allows courts with jurisdiction over the offense to issue search warrants for electronic communications stored by providers anywhere in the country) of the PATRIOT Act to rescue the girl and to track and prosecute the defendant, not Section 216 (which addresses the use of pen registers and trap-and-trace devices).

The Tyree case, however, does illustrate two of the ways in which the tools provided by the PATRIOT Act help to make Americans safer and contribute to successful prosecutions. Several days after the child's parents reported her missing in Pittsburgh, an anonymous caller told the FBI that he had chatted online with an individual who had taken a girl from Pittsburgh, and gave agents the individual's screen name. Within hours, pursuant to Section 212, FBI agents quickly obtained Tyree's name and home address, then immediately rescued the child victim from Tyree's home and arrested Tyree at his place of employment.

The Honorable Orrin G. Hatch
Page 2

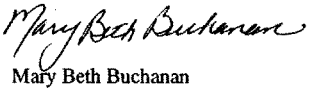
Before enactment of the PATRIOT Act, these agents could not have moved to rescue this child nearly as quickly because communications providers would not disclose such records in emergency situations for fear of civil liability. Section 212 eliminated this fear by giving these communications providers immunity from civil suit for assisting law enforcement in such cases.

In this same investigation, investigators also used Section 220 to quickly and efficiently obtain search warrants in one court in Pennsylvania for records of Tyree's e-mail and other electronic communications that were stored by multiple providers in California and Virginia. These records helped prosecutors build the case against Tyree by revealing his online conversations with the child victim before he took her to his home and sexually abused her. Before enactment of the PATRIOT Act, investigations were often delayed, and some courts were unduly burdened, by the requirement that individual warrants be obtained in each and every one of the districts where the communications providers were located.

As I stated at the hearing, Tyree was sentenced to nineteen years in prison for his conduct; more importantly, the child victim was rescued and safely returned to her family.

I respectfully request that this letter be added to the hearing record. I also hope to be able to supplement this letter at my earliest opportunity with further examples of the Department's use of Section 216 of the PATRIOT Act. I again thank the Committee for its continued leadership and support, and look forward to future discussions of the Department's efforts to combat pornography.

Sincerely,



Mary Beth Buchanan
U.S. Attorney for the
Western District of Pennsylvania

93014.198

Victor Cline, Ph D* Witness Statement on Pornography Effects:

U.S. Senate Committee Hearing on Child Pornography: Rm 226 Senate Office Bldg 15 Oct '03

My name is Victor Cline. I am a clinical psychologist and psychotherapist specializing in marital and family counseling and the treatment of sexual compulsions and addictions with a U.C. Berkeley Ph D. in psychology. I also work with the victims of sexual abuse and assault. Additionally I'm a behavioral scientist with approximately 85 publications some of which are in the area of "media violence and pornography effects." In the last 26 years I have treated approximately 350 male sexual addicts or compulsives including many pedophiles and their victims. I also treat rapists, voyeurs, fetishists, those making obscene phone calls, those compulsively promiscuous plus many other types of paraphilias. These sexual illnesses all have a common core and dynamic base. They are sexual in nature, highly addictive, compulsive and repetitive, very difficult to treat, where self-control and self discipline don't stop their occurrence. In other words there is a striking lack of "free agency" in the perpetrator. They do things that put themselves and their victims at great risk of harm.

The internet represents, in my experience, an area of significant risk for many children. Where parents have neglected to protect them with adequate filters on their home computers or with frequent access to computers in public libraries (most of which lack protecting filters) this makes it exceedingly easy for children to peruse via the internet explicit depictions of child-adult sex, rape, incest, bestiality, plus cyber warehouses filled with other depictions of sexual aberrations. I see too many patients of minor age who are stimulated to practice or try out in real life the things they see in this material. I see repeatedly older children sexually abusing younger children. In my judgment this represents a significant health hazard. Also: internet chat rooms can be particularly dangerous as a place for the seduction and enticement of children who are later "picked up" and molested by adult male pedophiles posing as children

Some of my patient perpetrators and sexual predators are middle aged men while others are teenage males who sexually abuse younger sisters or other younger more vulnerable children in the neighborhood. With most of them, I find, any kind of pornography, can act as an incitement to imitate it in real life with someone they have access to and can intimidate not to tell. Many of my perpetrators are also themselves victims with a history of being sexually abused by older predators at a previous time in their life. With a large majority of them an underlying thread is the use of child, adolescent, or adult pornography to stimulate their sexual appetites and provide models of sexual abuse as well as be used as tools to seduce new victims. In my experience its the child pornography that is the most malignant and poses the most risk to society..

The best evidence to date suggests that most or all sexual deviations are learned behaviors, usually through inadvertent or accidental conditioning. There is no convincing evidence, to date, suggesting the hereditary transmission of any pathological sexual behavior pattern such as pedophilia, rape, incest, exhibitionism, etc. In fact one British psychologist, Stanley Rachman demonstrated in the

93014.199

laboratory using live male subjects how easy it is to repeatedly condition normal males into a sexual illness or addiction. Another psychologist/researcher, R.C. McGuire, explains as a man repeatedly masturbates to a vivid sexual fantasy as his exclusive sexual outlet (introduced by a real life sexual experience or possibly pornography) the pleasurable experiences endow the deviant fantasy (rape, molesting children, etc.) with increasing erotic value. The orgasm experienced then provides the critical reinforcing event for the conditioning of the fantasy preceding or accompanying the act. McGuire indicates that any type of sexual deviation can be acquired in this way, that it may include several unrelated deviations in one individual and that it cannot be eliminated even by massive feelings of guilt. His paper cites many case histories to illustrate this type of conditioning. Other related studies by D.R. Evens and B.T. Jackson support his thesis. They found that deviant masturbatory fantasy very significantly effected the habit strength of the subject's sexual deviation.

Child pornography is particularly pernicious because the child victims (whether sexually abused while being photographed, or exposed to the pictures as part of their seduction) are relatively powerless (due to their young age and innocence, and immaturity) as well as not fully understanding the harm potential. Their frequent willingness to trust an older person who appears to be kind and accepting of them makes them more easy prey.

In my treatment of hundreds of primarily male patients with paraphilias (sexual pathology) I consistently have found that most men are vulnerable to the effects of masturbatory conditioning to pornography with a consequence of sexual ill health because we are all subject to the laws of learning with few or no exceptions. Not everyone gets addicted immediately, but if they persist in this behavior they will.

Researcher Patrick Carnes found that of 932 sex addicts studied 90% of the males said that pornography was significant to their addiction. (p 57, "Don't Call it Love", Bantom Books, 1991.)

In my experiences as a sexual therapist, any individual who regularly masturbates to pornography is at risk of becoming in time a sexual addict, as well as conditioning himself into having a sexual deviancy. In time the "high" obtained from masturbating to pornography becomes more important than real life relationships. It makes no difference if one is an eminent physician, attorney, minister, athlete, corporate executive, college president, unskilled laborer, president of the U.S. or an average 16 year old boy. All can be self conditioned into deviancy.

The process of masturbatory conditioning is inexorable and does not spontaneously remiss. The course of this illness may be slow and is nearly always hidden from view. It is usually a secret part of the man's life, and like a cancer, it keeps growing and spreading. It rarely ever reverses itself, and it is also very difficult to treat and heal.. Denial on the part of the addict and refusal to confront the problem are typical and predictable. The presence of child pornography creates the potential of many

types of harms in the community including helping to create sexual predators or pedophiles and later their victims.

In the case of pedophiles, the overwhelming majority, in my clinical experience use child pornography and /or create it to stimulate and whet their sexual appetites which they masturbate to then later use as a model for their own sexual acting out with children. I find that the use of child pornography in time desensitizes the viewer to its pathology no matter how aberrant or disturbing. It becomes acceptable and preferred. The man always escalates to more deviant material, and the acting out continues and escalates despite very painful consequences such as destruction of the family, loss of spouse, children, job, health, or incarceration after committing criminal acts.

Some also use it to seduce children into engaging in sexual acts with themselves. When they introduce it to children the suggestion is that this is normal behavior and many other young people, like themselves, also use it and do these things.. Pedophiles often trade, lend, or sell the pictures they make of young people nude and having sex through an informal network. Some of the pornography they accumulate is of females fully developed anatomically but made to look young and immature by dressing them in children's clothes and arranging their hair--such as with a pony tail--to suggest to the viewer that they are underage minors when in fact they may not be. While the producers of this material may claim that no underage children were used in producing this pornographic material--to the viewer this is irrelevant because they are *perceived* as minors by the psyche and this erotic arousal generalizes to all potential real-child victims.

1. Rachman, S. "Experimentally induced sexual fetishism" *Psychological Records*, 1968, vol 18, p.. 25. 2. McGuire, R.J., et al. "Sexual Deviations as Conditioned Behavior: A Hypothesis." *Behavior Research & Therapy*, 1965, vol 2, p. 185. 3. Evans, D. R. "Masturbatory Fantasy & Sexual Deviation". *Behavioral Research & Therapy*, 1968: vol. 6, p 17. 4. Jackson, B.T., "A Case of Voyeurism Treated by Counter Conditioning." *Behavior Research & Therapy*, 1969, vol 7, p. 133.

Dr. Victor Cline is a Univ. of Calif. Berkeley Ph D in Psychology, later a Research Scientist with the George Washington University's Human Resources Research Office, and currently an Emeritus Professor in Psychology at the University of Utah. His private clinical practice is in Salt Lake City, Utah.

FURTHER DOCUMENTATION OF PORN EFFECTS"

1. CAUGHT IN THE NET. How to Recognize the Signs of Internet Addiction and a Winning Strategy for Recovery. by K. Young (1998). New York: John Wiley & Sons Publ.

2. CONTRARY TO LOVE: Helping the Sexual Addict. By P. Carnes (1989) Minneapolis: CompCare Publishers.

3. CYBERSEX EXPOSED. by J. Schneider & Robt. Weiss. (2001) Center City, Minn. Hazelden Publ.

4. CYBERSEX UNHOOKED: A Workbook for Breaking Free of Compulsive Online Sexual Behavior. By D. Delmonico, et al. (2001) Wickenburg, Az. Gentle Path Press

5. DON'T CALL IT LOVE: Recovery From Sexual Addiction. By P. Carnes. (1991) New York: Bantam Books

6. DRUG OF THE NEW MILLENIUM: The Science of How Internet Pornography Radically Alters the Human Brain & Body. By M. Kastleman. (2001). Orem, Ut. Granite Publishing.

7. HOPE & RECOVERY: A Twelve Step guide for Healing from Compulsive Sexual Behavior. (many authors) (1987) Center City, Minn. Hazelden. Publ.

8. FACING THE SHADOW: Starting Sexual & Relationship Recovery (A Gentle Path Workbook for Beginning Recovery from Sex Addiction)". By P. Carnes. (2001) Wickenburg, Arizona: Gentle Path Press.

9. IN THE SHADOWS OF THE NET: Breaking Free of Compulsive Online Sexual Behavior. By P. Carnes et al. (2001) Center City, Minn. Hazelden Publ.

10. LONELY ALL THE TIME: Recognizing, Understanding, & Overcoming Sex Addiction, for Addicts & Co-Dependents. By R. Earle & G. Crow. (1989) New York: Pocket Books.

11. OUT OF THE SHADOWS: Understanding Sexual Addiction. By P. Carnes (2001) Center City, Minn. Hazelden

12. PORNOGRAPHY EFFECTS ON ADULTS & CHILDREN. By V. Cline, (2001) New York: Morality in Media

Department of Justice

STATEMENT

OF

THE HONORABLE J. ROBERT FLORES
ADMINISTRATOR
OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION
OFFICE OF JUSTICE PROGRAMS

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

REGARDING

INDECENT EXPOSURE: OVERSIGHT OF THE EFFORTS OF THE DEPARTMENT OF JUSTICE TO PROTECT PORNOGRAPHY'S VICTIMS

PRESENTED ON

OCTOBER 15, 2003

Mr. Chairman, Senator Leahy, and Members of the Committee: I am J. Robert Flores, Administrator of the Office of Juvenile Justice and Delinquency within the Department of Justice's Office of Justice Programs. On behalf of the Office of Justice Programs, I am grateful to have the opportunity to testify before you today on the subject of the Department's efforts to protect the victims of pornography.

The Office of Juvenile Justice and Delinquency Prevention (OJJDP) continues to commit resources to protect children and families from the harms associated with sexual exploitation, sexual abuse, child pornography, and sexual predators. Historically, OJJDP has provided that assistance through its administration of funds provided by Congress to develop and provide technical assistance, training to law enforcement and prosecutors on the state and local levels, and public education programs that disseminate methods and programs that work to keep kids safe. I want to assure you that this commitment has never been stronger, and, as I will detail for you, help that the President and Attorney General have publicly committed to providing is being expanded for children and families.

The Internet Crimes Against Children Task Forces

OJJDP has tackled child pornography and computer-facilitated child sexual exploitation since 1998 when we identified and funded the first ten Internet Crimes Against Children (ICAC) Task Forces. Last year, the President sought and obtained from Congress additional funding to assure that the Task Forces could provide nationwide coverage. There are now 40 Task Forces, which have become regional clusters of technical and investigative expertise that offer

93014.203

prevention and investigative services to children, parents, educators, law enforcement officers, and other individuals working on child sexual exploitation issues. The theory behind the ICAC Task Forces is well understood and has been repeatedly tested in other law enforcement arenas and found to work. Simply put, by combining law enforcement personnel from local, state, and federal agencies so that jurisdictional and technical barriers can be overcome and subject matter expertise can be accessed quickly and efficiently, ICAC Task Forces draw upon the combined strengths of each participating agency, thereby overcoming any individual weaknesses.

The ICAC Task Force program is not a luxury but a necessity because predators, pornographers, and promoters of material harmful to minors continue to exploit new computer technologies to advance their own goals. Moreover, unlike some adults who view the benefits of the Information Age dubiously, children and teenagers have seized upon the Internet's educational and recreational capabilities with astonishing speed and casualness and will continue to do so. Adapting information technology to meet everyday needs, young people increasingly go online to meet friends, satisfy information needs, purchase goods and services, and complete school assignments. Currently, 28 million children and teenagers have access to the Internet, and industry experts predict that they will be joined by another 50 million globally by 2005. Although the Internet gives children and teenagers access to civilization's greatest museums, libraries, and universities, it also increases their risk of being sexually exploited or victimized.

Large numbers of young people encounter sexual solicitations they do not want and sexual material they do not seek. In the most serious cases, they are targeted by offenders

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00283 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.204

seeking children for sex. Research conducted by the University of New Hampshire reveals that one in five children between ages of 10 and 17 received a sexual solicitation over the Internet in 1999. One in 33 received an aggressive solicitation from a stranger who asked to meet them somewhere, called them on the telephone, or sent them mail, money, or gifts. As my colleague, Mr. Malcolm, has stated in his written testimony, the percentage of children touched and thereby harmed by pornographic material is now higher than in 1999 and continues to grow.

Cloaked in the anonymity of cyberspace, sex offenders can capitalize on the natural curiosity of children and seek victims with little risk of detection. Preferential sex offenders no longer need to lurk in parks and malls. Instead, they can roam from chat room to chat room, trolling for children susceptible to victimization in that child's own bedroom. This alarming activity has grave implications for parents, teachers, and law enforcement officers because it circumvents conventional safeguards and provides sex offenders with virtually unlimited opportunities for unsupervised contact with children.

Today's Internet has also become the new marketplace for offenders seeking to acquire material for their child pornography collections. More insidious than the exchange of sexually explicit material among adults, child pornography depicts the sexual assault of children and is often used by child molesters to recruit, seduce, and control future victims. Pornography is used to break down inhibitions, validate sex between children and adults as normal, and control victims throughout their molestation. When offenders lose interest in their victims, pornography is often used as blackmail to ensure the child's silence. When posted on the Internet,

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00284 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.205

pornography becomes an enduring and irretrievable record of victimization and a relentless violation of that child's privacy.

OJJDP recognizes that the increasing online presence of children, the proliferation of child pornography, and the lure of predators searching for unsupervised contact with underage victims present a significant threat to the health and safety of children, and a formidable challenge for law enforcement today and into the foreseeable future. Many factors complicate law enforcement's response to these challenges. Conventional definitions of jurisdiction are practically meaningless in the electronic universe of cyberspace, and very few investigations begin and end within the same jurisdiction. Because they involve multiple jurisdictions, most investigations require close coordination and cooperation among federal, state, and local law enforcement agencies.

The National Center for Missing and Exploited Children's (NCMEC) Cybertipline, launched March 9, 1998, assists law enforcement with the identification of online predators and those who would sexually exploit children. It also serves as the national clearinghouse for tips and leads about child pornography and child sexual exploitation. Additionally, NCMEC launched Cybertipline II to handle child pornography leads reported by the electronic service providers. These reports are available online in "real time" only to the Federal Bureau of Investigation (FBI), the Bureau of Immigration and Customs Enforcement (ICE), and the ICAC Task Forces.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00285 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.206

It is clear, as evidenced by the data in NCMEC s Quarterly Progress Report submitted to OJJDP for the third quarter of Fiscal Year 2003, that the flow of child pornography complaints has not slowed down since the Cybertipline was launched in March 1998. In fact, according to NCMEC, more than 21,000 complaints of child pornography were reported to the Cybertipline from July 2003 to September 2003. That brings the total number of reports to the Cybertipline to more than 150,000. While the total figure is staggering in and of itself, 21,000 complaints occurred in the third quarter of Fiscal Year 2003 alone, representing nearly 15 percent of the total child pornography complaints.

The cooperative efforts of NCMEC's Electronic Crimes Unit and the Louisiana Attorney General's Office ICAC Task Force, funded by OJJDP, recently brought to closure a case that represents the impact of just one cybertip. In this particular case, an ex-Navy officer was found to have "hundreds and hundreds" of child porn images stored and organized by age on his computer. The suspect, who was also involved in the local school district and owned his own computer company, was arrested in July 2003 on one count of possession of child pornography.

As in the example above, NCMEC figures only represent actual reports of child pornography submitted to the Cybertiplines. Unfortunately, there is no way to quantify the full scope of the child pornography issue because there is no way to know how much undocumented child pornography exists.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00286 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.207

Without a doubt, the pervasiveness of the child pornography problem is enormous. However, there is a tremendous amount of work being conducted by law enforcement and prosecutorial agencies at the federal, state, and local levels. Within the Department of Justice alone, three separate entities, OJJDP, through the ICAC Task Forces; the Child Exploitation and Obscenity Section (CEOS) of the Criminal Division; and the FBI's Innocent Images Initiative, are spearheading multi-agency, multi-jurisdictional efforts to stem the tide of child pornography.

The new Predator initiative developed by the Department of Homeland Security's (DHS) Bureau of Immigration and Customs Enforcement is working hand-in-hand with the Department of Justice to protect children worldwide. This comprehensive DHS program will identify child predators and remove them from the United States (if subject to deportation). Operation Predator will also work to identify children depicted in child pornography to help rescue them, and assist U.S. Attorneys in developing cases and prosecuting the people responsible for making and distributing the pornographic material. Also within DHS, the United States Secret Service (USSS) is expanding its Forensic Services Division to assist with cases involving missing and sexually exploited children.

Finally, the long-standing work of the U. S. Postal Inspection Service (USPIS) is ever present in addressing cases pertaining to child pornography and child exploitation.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00287 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.208

While the work completed by these federal, state, and local agencies is impressive, it demonstrates a level of improved cooperation and coordination that is even more impressive. At all levels, and in concert, law enforcement is tackling the child pornography issue aggressively. A new sense of teamwork and joint ownership of the problem has emerged to pursue child pornographers ranging from the lowly collector to the most heinous of offenders who would manufacture and distribute child pornography images.

An excellent example of this cooperative spirit is reflected in the creation of a National Child Victim Identification System. In an unprecedented partnership with NCMEC, the FBI, the USPIS, USSS, the ICAC Task Forces and CEOS, ICE's CyberSmuggling Center hosts the nation's only comprehensive, searchable system for identifying digital child pornography images. With its capacity to search and identify known images, the system is designed to help law enforcement agencies throughout the world identify and rescue children featured in child pornography, and facilitate prosecution of those who possess or distribute digital child pornography images in the wake of a 2002 Supreme Court decision (*Ashcroft v. Free Speech Coalition*) requiring proof that such images depict an actual child. Because the effort leverages a comprehensive partnership among federal, state, and local law enforcement agencies, this system will eventually contain all known child pornography images on the Internet. Already, the ICE CyberSmuggling Center has positively identified children featured in roughly 300 images and has provided this information to law enforcement agencies nationwide for prosecutorial purposes.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00288 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.209

With improved coordination, successful arrests and prosecutions are being reported daily. In fact, the 40 OJJDP-funded ICAC Task Forces alone have been responsible for more than 1,500 arrests in the past five years, with nearly 500 of those taking place in just the past 12 months. In addition to these arrests, the ICAC Task Forces have made nearly 2,600 case referrals to non-ICAC law enforcement agencies. Of the 14,000 cases the ICAC Task Forces have been involved with in the past five years, either through actual investigations, referrals or technical support, nearly 11,000 of those cases have been directly related to the possession, distribution, or manufacturing of child pornography. There is no question that the ICAC Task Force program has made an indelible mark in the battle against child pornography and child exploitation. In response to President Bush's October 2002 directive at the White House Conference on Missing, Exploited, and Runaway Children, OJJDP is further expanding the ICAC Task Force program and, by Winter 2004, will have 45 state and local ICAC Task Forces in place and operational.

Next steps in combating child exploitation

With all of our success in arresting and prosecuting predators, the reality is that child pornography is only one component of the broader child exploitation issue. Another key element is the targeted distribution of obscene material to children. This alarming trend is intended to have a twofold impact. First, as noted previously, child pornography depicts the sexual assault of children and is often used by child molesters to recruit, seduce, and control future victims. However, predators do not use child pornography in all cases, but instead, send obscene, possibly adult, pornography to children. Predators employ these same tactics to break down a child's

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00289 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.210

barriers and desensitize them as a means to lure and seduce them into sexual exploitation.

Secondly, the distribution of obscene material to children is the commercial porn industry's vehicle to create a new generation of pornography "junkies" drawn to commercial Web sites through the manipulation of common and well-known children's Web site names. This disturbing trend was recently reflected in charges filed by the U. S. Attorney for the Southern District of New York, when, in September of this year, a suspect was arrested in his Florida hotel room on charges arising from his alleged creation and use of misleading domain names on the Internet to deceive minors into logging onto pornographic Web sites. The activity allegedly brought the suspect as much as $1 million a year, paid by the commercial porn industry for every hit directed to their sites.

In light of this reality, it is my considered judgment that it is critical to fulfill the President and Attorney General's mandate to address not only the worst of these predators and exploiters, but also those who deluge children and families who use the Internet with illegal and unwanted pornography. Today, the Internet is so polluted that it is difficult to pick out a single item of garbage. The amount, types, and frequency have left many children and parents feeling overwhelmed. Moreover, as the pornographic morass has grown, it is now much easier for a predator to find a place to hide amid the garbage. The decision to allow Internet pollution to grow and with it the sense that anything goes, has cost our children a great deal. Thus, we must begin to look at all illegal activity on the Internet and send a clear signal that the law does apply to this critically important medium and that we will not abandon the Internet to those who would

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00290 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.211

abuse it.

In response, OJJDP has undertaken a program that we will build together with other Justice Department components and other agencies that have a direct and strong interest in protecting children and families.

First, the Department has directed the ICAC Task Forces to include, as a part of their investigative efforts, a new focus on adult obscenity cases when a child is the target of the obscene material or where such material has been used to seduce or facilitate the exploitation or abuse of a child. While case prioritization is and must be given to life threatening situations or when imminent danger of continued physical and/or sexual abuse is present, obscene material directed at children should be viewed as an important and potential precursor to real physical or sexual abuse. Most important, however, is the fact that we cannot protect children if we do not change the environment on the Net from one where predators flock with an expectation of safety to one where they surf or troll at their peril.

As with most deviant behavior, arresting and prosecuting offenders will not alone solve the problems of child pornography and sexual exploitation. On the contrary, as the number of homes with Internet access continues to increase, the pool of potential victims correspondingly grows. Likewise, children cannot but help reach the dangerous conclusion that obscenity must be okay if we, the adults responsible for their safety, allow it to grow unabated and continue to send them into this environment. Like any successful effort to change expectations and behavior, we

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00291 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.212

must send consistent messages on every front and not merely be content to say, through our actions, that we will respond only when it directly threatens the immediate physical safety of a child. Our children are simply owed more.

The decision to ask the ICAC Task Forces to take on this responsibility flows naturally from the direction the President has provided: Build once, use many times. These task forces already possess the forensic and computer skills to undertake obscenity investigations. Their membership includes local and state investigators who are familiar with the local community standards and have relationships with local and state investigators in other task forces with whom they can work when the obscenity case at issue begins or ends in another jurisdiction. Finally, it is imperative that we shepherd federal investigative and prosecution resources carefully so that where appropriate cases are developed, they can be referred for federal prosecution, keeping in mind that the protection of our citizens from the harms caused by obscenity and pornography must remain a state and local responsibility as well. By extending the ICAC task force reach, we allow them to go where the evidence leads and not ignore viable prosecutions and investigations. Finally, if each task force opened only three to five cases in the next 12 months, that would result in an increase of 135 to 225 cases nationwide. By taking small steps together, task forces can substantially enhance the efforts of the Criminal Division and the U. S. Attorneys.

Even as we begin to send a clear message that obscenity investigations will increase, we must also work to encourage parents, teachers, businesses, and the faith community to shoulder a greater share of responsibility to work to create a safe and supportive Internet environment for

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00292 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.213

our children. As I travel throughout the country speaking to law enforcement, children, Internet service providers, and Internet safety experts, they all tell me that they continue to struggle with the question of how to engage adults, especially parents, on issues of Internet safety. Most, if not all, of the education efforts to protect children have been directed to children and teens. Congress has passed several statutes addressing corporate activities connected to the distribution of pornography, and libraries and schools have had their funding of Internet access conditioned on taking significant steps to protect children. While we are beginning to see progress on these fronts, parents continue to be the missing cog and they remain the best way to protect children. We must make progress on this front.

OJJDP will focus on efforts to engage and involve parents, as part of a comprehensive strategy that takes advantage of where we are today and addresses the reality of current demands on parents, children, corporate America, schools, and our nation's safety.

In March 2002, OJJDP hosted an Internet Safety Focus Group that brought together government officials and representatives from private corporations and non-profit organizations to discuss the increasing number of children and teenagers using the Internet, the proliferation of child pornography, and the heightened activity by predators searching for unsupervised contact with underage victims. During the day-long session, the group concluded that it is critical to address computer-facilitated child exploitation, which presents a threat to the health and safety of young people, and is a formidable challenge for parents, teachers, and professionals in law enforcement and youth service agencies. However, there was consensus that child exploitation

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00293 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.214

was endemic of broader social issues concerning the Internet and its use. In short, the group concluded that significant areas of concern remain that have not been adequately addressed.

First, although education about the problem is extensive and law enforcement efforts have never been greater, our country has continued to lose ground to predators, pornographers, and others who seek to harm our children, as reflected in NCMEC's report.

Second, in spite of aggressive law enforcement efforts, law enforcement resources pale in comparison to those of the population that is set on exploiting children or polluting the Internet that our children use, resulting in new forms of exploitation and danger.

Third, despite widespread information in the media, through schools, and commercial marketing, which warns of the risks of unsupervised Internet use, parents have failed to substantially increase their involvement in their children's Internet use or utilize danger-reducing technologies.

Finally, even where efforts have been made by parents, students, schools, communities, or law enforcement, these efforts have lacked coordination and, as a result, have been only moderately successful at best.

With the number of households connecting to the Internet increasing yearly, coupled with the populations of preteens and teenagers burgeoning in the next five to ten years, it is now time

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00294 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.215

to develop a strategy for the future of Internet Safety. OJJDP has taken the first step by convening the focus group. OJJDP believes that the problem of Internet-based obscenity, child exploitation, and other related dangers is one that has numerous causes and that any successful effort must have the participation of multiple agencies.

To move forward, I have scheduled a meeting on November 4, 2003, with officials from the Departments of Education, Commerce, and Health and Human Services, as well as key policymakers from four select user communities, to create and develop an approach targeting this broad issue. OJJDP, in partnership with the other agencies, will pursue lowering the risk of abuse or exploitation to children using the Internet. Metrics to determine whether such a goal is being met will include determining whether children face increased difficulty in obtaining material that is harmful to them whether intentionally or not; whether or not there is a lower incidence of illicit or illegal activity reported by industry serving the local community; if there is a greater likelihood of discovery of illegal activity as a result of easier reporting, better forensic tools; and if the number of reported Internet-based offenses is reduced.

Local partners in the select communities will include schools, parent/teacher organizations, business, law enforcement, computer/Internet industry, and the faith community. Jointly, we will explore the best models for attacking the pervasiveness of child pornography and child exploitation and continue to work diligently to bring it to an end.

I have great confidence that this effort can succeed because we stand in a different place

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00295 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.216

than we did even a year ago. Today, corporate America has recognized, perhaps in a way it wished it did not, that an environment of lawlessness and an inability of Internet users to properly translate how law operates from the real world to the cyber world, also puts corporate America in jeopardy. I think that corporations are now ready to work in a different way to support safety and law on the Net. Parents now recognize, as they have with underage drinking, that conduct they facilitate might cost them personally. And, educators and librarians now see that there are constitutional limits that can properly be placed on the use of taxpayers' hard earned money. Finally, to those of us who have been in the battle to protect children, we have come to understand that it is the adult's responsibility to protect a child, and while we have many ways to do this, failure to accomplish that goal lies squarely at the feet of the adult community.

I am encouraged that we are here today and that much progress has been made. I look forward to reporting back how we give life to the President's direction and the Attorney General's decision to once again pursue an Internet that is safe for children and families.

This concludes my statement. I welcome the opportunity to answer any questions that Committee members may have.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00296 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.217

STATEMENT OF SENATOR CHARLES GRASSLEY
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

INDECENT EXPOSURE: OVERSIGHT OF THE EFFORTS OF THE DEPARMENT OF JUSTICE TO PROTECT PORNOGRAPHY'S VICTIMS

OCTOBER 15, 2003

Mr. Chairman, thank you for holding today's oversight hearing on the federal government's - in particular the Justice Department's - efforts to protect innocent children and for that matter adults from the scourge of illegal pornography. Hardly a week goes by that I don't receive a letter from an Iowan concerned about pornography and its harmful impact on his or her family. My constituents want to know what the government and the Congress are doing about all the smut that invades their homes by way of the Internet and cable television. So, I want you to know that I appreciate your holding today's hearing to answer my constituents'– and I am sure, all of our constituents'– concerns.

It seems that since the early to mid 1990s, Congress has made some valiant attempts to pass Constitutional protections for children using the Internet. So far we have a mixed record. The Supreme Court has overruled one of our bills, the Communications Decency Act, which tried to protect children from indecent material on the Internet. It's upheld one, the Children's Internet Protection Act, which requires public libraries and schools to install Internet filters on their computer stations. And, just yesterday, the Court agreed to take up another, the Child Online Protection Act, which if upheld – and I'm optimistic that it will be – will shield children from material that is "harmful to minors" while they surf the Internet. I supported each of these bills and I'm glad that I did.

During the last ten years the obscenity and child pornography industry has grown by quantum leaps. It's no coincidence that during that same time the Department of Justice did preciously little in the area of obscenity prosecution. By all accounts, the Reno Justice Department brought no more than a hand full of obscenity prosecutions. I'm forced to believe that this laxity toward this area of federal criminal law has contributed to the "wild west" environment of the Internet.

93014.218

Unfortunately some have been critical of the current Administration for being slow out of the gate with regard to the enforcement of the federal obscenity laws. I don't know whether that is the case or not, but I'm glad that the Department of Justice can be here today to discuss their efforts. It's my understanding that the investigation and prosecution of these crimes is complex and time consuming and is further complicated when the Internet is used to distribute the obscene material. I look forward to hearing the testimony of our Department of Justice and Postal Service witnesses.

In reviewing the testimony, I was particularly glad to hear about the Office of Juvenile Justice and Delinquency Prevention's Internet Crimes Against Children Task Forces (ICAC) initiative. I think that it is wise to use the ICACS to leverage state and local resources in the effort to protect children from obscenity as well as child pornography.

There is substantial evidence that obscenity is not a victimless crime. According to the report of the Child Online Protection Act Commission, obscenity is a tool used by molesters in child molestation and exploitation. I also agree with Administrator Flores in his assertion that distributors of obscenity, especially on the Internet, target children with deceptive sounding website names, so that they may reach their next generation of users. The illegal pornography industry is big business and our children are paying the greatest cost for these criminals' commercial success.
Because of the harm that obscenity poses for minors, it is critical that the ICACs be given technical assistance and training in how to investigate and prosecute federal obscenity crimes as well, as child pornography. By arming state and local investigators and prosecutors, we will be enlisting an army in the effort to protect women and children from exploitation.

The Committee will be hearing from a knowledgeable and experienced second panel. Their testimony will be essential to our full understanding of how people can be protected from the harms of obscenity and child pornography. I'm glad Dr. Victor Cline could be with us this afternoon. He has a long and distinguished career of research into and treatment of the harms that obscenity and child pornography cause. It's also good to see Bruce Taylor from the

93014.219

National Law Center for Children and Families. He has worked with the Judiciary Committee a number of times in the past. I'm sure that he will be able to give the Committee a good perspective on the history of obscenity prosecution, and maybe even some advice on how we can best attack this criminal problem. I also want to thank Detective Takeshita for his years of service on the Los Angeles Police Department. He will be able to give the Committee some helpful insight into how big this problem is.

Mr. Chairman, I want to thank you again for holding this hearing and for your commitment over the years to protecting children from the harms of illegal pornography.

News Release

JUDICIARY COMMITTEE

United States Senate • Senator Orrin Hatch, Chairman

October 15, 2003 Contact: Margarita Tapia, 202/224-5225

Statement of Senator Orrin G. Hatch
Before the United States Senate Judiciary Committee
Hearing on

"INDECENT EXPOSURE: OVERSIGHT OF DOJ'S EFFORTS TO PROTECT PORNOGRAPHY'S VICTIMS"

Good afternoon. Today we will be conducting an oversight hearing on the Department of Justice's Efforts to Prosecute Child Pornography and Obscenity. As many of you know, pornography is a growing problem in America. For example, in a recent *ABC Primetime Thursday* story, Diane Sawyer stated that the pornography industry is estimated at $10 billion, which is bigger than the NFL, NBA and Major League Baseball combined. And it's getting worse with the advent of the Internet. Pornographic web pages now top 250 million and are growing at an unprecedented rate. It is estimated that porn on the Internet will grow to become a $7 billion industry in the next five years – unless we have aggressive law enforcement.

The National Society for the Prevention of Cruelty to Children estimates that there are 140,000 images of *child* pornography online. The typical age of children depicted in these images is between 6 and 12, but the profile is getting younger.

In addition, *adult* pornography has become readily available to minors. There are currently 28 million children and teenagers with access to the Internet and an additional 50 million globally are estimated by 2005. Nine out of ten children, ages 8-16, have viewed pornography online, mostly unintentionally, and when using the Internet to do homework. And those children who seek it out of curiosity have no trouble getting it. 97 percent of adult web sites do not require adult verification.

The result of all this porn is that there are 11, 12, or 13-year old children being treated for pornography addictions. As Professor Victor Cline previously testified before the Child Online Protection Act (COPA) Commission, the overwhelming majority of pedophiles use child pornography to stimulate and whet their sexual appetites before abusing children. They also use child porn to desensitize children and lure them into participating in sexual activity. In addition, as the *ABC Primetime Thursday* piece made clear, the victims of pornography are not just addicts and rape victims -- but young, innocent teenagers, who go to Los Angeles with dreams of becoming a movie star and instead get caught up in this sordid industry.

I have always believed very strongly in protecting children from this type of offensive material. I sponsored the PROTECT Act, which the President enacted six months ago. This is

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00300 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.221

one of the most significant pieces of child crime legislation that Congress has passed in recent years. It gives law enforcement the tools it needs to effectively prosecute child pornographers. In addition to authorizing criminal prosecutions of child pornographers, the Act provided funding for more prosecutors and investigators, and established a cyber tip-line to report on-line child exploitation. It also created a national registry of child pornographers.

I am currently considering legislative solutions to the many risks inherent in the use of peer-to-peer networks. Almost half of the people who use these networks are minors. Recent studies have shown that millions and millions of pornographic files are available for downloading on these networks at any given time. Even more disturbing is that searches on these networks using search terms that a child would be expected to use, such as Harry Potter or Pokemon, turn up an enormous percentage – over 50% in one study according to the GAO -- of pornographic materials including child pornography. This is simply unacceptable. Many parents – possibly the majority of them – are unaware of this problem. I think this requires our immediate attention.

I look forward to hearing about DOJ's efforts to combat both child pornography and obscenity. This is a growing problem that we need to attack aggressively. We cannot sit quietly and hope it will go away.

The hearing today will consist of two panels. The first panel includes three representatives from the U.S. Department of Justice – John Malcolm, Deputy Assistant Attorney General of the Criminal Division, J. Robert Flores, Administrator of the Office of Juvenile Justice and Delinquency Prevention, and Mary Beth Buchanan, U.S. Attorney for the Western District of Pennsylvania. In addition, we have Lawrence Maxwell, Inspector-in-Charge from the Postal Inspection Service.

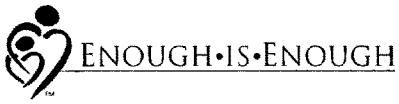
The second panel consists of Bruce Taylor, President and Chief Counsel of the National Law Center for Children and Families, Detective Steve Takeshita, Officer in Charge of the Pornography Unit in the Los Angeles Police Department and Emeritus Professor from the University of Utah, Dr. Victor Cline. Welcome to the hearing and I look forward to listening to your testimony.

In addition, at this time, I would like to submit for the record, the written testimony of Donna Rice Hughes, President of *Enough is Enough,* and an advocate of protecting children from pornography on the Internet.

# # #

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00301 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.222



U. S. SENATE
JUDICIARY COMMITTEE

Illegal Pornography and the Internet

October 15, 2003
Written Testimony By
Donna Rice Hughes
President, Enough Is Enough

746 Walker Road, Suite 116 • Great Falls, Virginia 22066
www.enough.org • fax 703.759.3810
www.protectkids.com

93014.223

10/14/03

U. S. SENATE
JUDICIARY COMMITTEE

ILLEGAL PORNOGRAPHY &
THE INTERNET
October 15, 2003
Written Testimony By
Donna Rice Hughes
President, Enough Is Enough

Donna Rice Hughes Biography

- President, Enough Is Enough
- Author, Kids Online: Protecting Your Children in Cyberspace (Revell, 1998)
- Child Online Protection Act (COPA) Commissioner (1998-2000)
- Founder – www.protectkids.com and www.enough.org
- Internet safety speaker and advocate

2

Enough Is Enough (EIE)

- Our mission is to make the Internet safer for children and families.
- Our strategy involves a three-pronged approach of shared responsibility between the public (parents, schools and libraries), the technology industry, and the legal community (law enforcement and public policy).
- EIE is a national, non-partisan, non-profit organization (501c3).

3

OVERVIEW

- The World Of CyberSex
  - What's happening?
- Just Harmless Fun?
  - Why should we care?
- The Search For Solutions
  - What should we do?

4

THE WORLD OF CYBERSEX

INDUSTRY

5

Cyber-Porn Beginnings

- Early 90's/Bulletin Board Services/ Newsgroups
- Barriers of access to all types of sexually-explicit material is virtually obliterated by the Internet
  - Anonymity
  - Ease of Access
  - Porn of choice (including black-market porn)
  - Inexpensive
  - Under law enforcement detection

6

Prepared by Donna Rice Hughes

93014.224

10/14/03

National Research Council Independent Study, 2002

- Large amounts of very graphic sexually explicit content on the Internet
- Easy to access
- Can stumble across it inadvertently
- Intrusive tactics used by pornographers to trick unsuspecting people (spam, mousetrapping, etc)
- Some would have been prosecuted if in print under past policy
- Some more graphic and shocking than what is easily available through non-Internet sources

(National Research Council, (NRC) Independent Study, 2002)

7

THE CYBERSEX INDUSTRY

Scale

- Generates approximately $1 billion annually
- Expected to grow to $5-7 billion over next 5 years, barring unforeseen change (enforcement)
- Total Adult Industry- current revenues estimated to be from $4 billion to $10 billion (NRC, 3-1, 2002)

8

THE CYBERSEX INDUSTRY

- Pornographic web pages now top 260 million and growing at an unprecedented rate (NRC, 9/23/03)
- 14 million identified pages of pornography in N2H2's database in 1998; growth to 260 million represents an almost 20-fold increase in just 5 years (NRC, 9/23/03)

9

THE CYBERSEX INDUSTRY

Structure

- Subscription sites exceed 100,000 in U.S. operated by about 1,000 U.S.-based firms
- The two largest individual buyers of bandwidth are U.S. firms in adult online industry
- Structure of industry consists of small number of large firms and larger number of small firms (NRC, 3-1, 2002)

10

FOLLOW THE MONEY

Online Porn Revenue Generated by the following:

- Consumer sales
- Mousetrapping- Pornographers receive referral fee
- Internet Advertising Models (NRC, 3.3, 2002)
  - CPA model-Cost per acquisition
  - CPC model-Cost per click
  - CPM model- Cost per million

  (CPM, CPC, & Mousetrapping Models have no incentive to distinguish between child and adult traffic. It's a numbers game) (NRC, 2002)

11

FUTURE TRENDS

- Due to saturated market:
  - More aggressive marketing
  - Incentives to niche market
  - Well-established firms testified sex sites becoming more specialized to accommodate any preference or extreme material as route to future growth (NRC, 3.5, 2002)

12

Prepared by Donna Rice Hughes

10/14/03

Free "Teaser" Images

- 74% of adult commercial sites display free teaser porn images on homepage, often porn banner ads
- 66% did not include a warning of adult content
- 11% included such a warning but did not have sexually explicit content on homepage
- 25 % prevented users from exiting site (mousetrapping)
- Only 3% required adult verification (COPA will remedy)

(Child-trading on the World wide Web: A Survey of Adult Webtrafficers, 1001. Interactive, NRC, 2002)

13

Porn-Napping and Hijacking

- 40,000 expired domain names porn-napped *(created a porn site in place of expired site)* or hijacked *(re-routed to existing porn site)*
- New owners offer re-sale $500-2,000 to expired domain prior owners (NRC, 2002)
- Hijacked to porn or gambling sites (Agency Trance Force, 3/2002)

14

Deceptive Marketing Practices

•Misspelled Words- (shareware vs. sharware)

•Innocent Word Searches- (toys, boys, pets, etc.)

•Stealth Sites- (whitehouse.com; coffeebeansupply.com; teenagershideout.com; http://clothingcatalog.com; watersports.com)

•Brand Name Misuse (Disney, Nintendo, Barbie, Levis, etc.)

•Unsolicited email - Spam

15

Pornographers' Use of Brand Names

- 26 popular children's characters, such as Pokemon, My Little Pony & Action Man, revealed thousands of links to porn sites
- 30% were hard-core (Internet, 2000)
- 25% of porn sites are estimated to use popular brand names in search engine magnets, metatags and links - Disney, Nintendo, and Barbie (Cyberwatch Survey, 1999)

16

CHILD PORNOGRAPHY

- 140,000 images of child pornography online (National Society for the Prevention of Cruelty to Children, 10/8/03)
- More than 20,000 child porn images posted every week (National Society for the Prevention of Cruelty to Children, 10/8/03)
- More than half of the child porn sites reported to Internet Watch Foundation are hosted in the U.S. (National Criminal Intelligence Service, 8/31/03)

17

CHILD PORNOGRAPHY

- 20 children are estimated to have been abused for first time/more than 1000 images of each child created (National Society for the Prevention of Cruelty to Children, 10/8/03)
- More babies and toddlers are appearing on the net and the abuse is getting worse. It is more torturous and sadistic than it was before. The typical age of children is between 6 and 12, but the profile is getting younger. (Combating Paedophile Information Networks in Europe, March 2003)

18

Prepared by Donna Rice Hughes

10/14/03

CHILD PORNOGRAPHY SPAM

- Child Porn Spam Increase
- Children at risk because they:
  - -are less careful online
  - -use chat rooms where their email addresses are collected by unknown people

(OCMEC, Press Pass, 12/15/01)

19

ONLINE OBSCENITY

- Watersports.com
  - -"Extreme pee and urination fetish site"
  - - Streaming video
- Boys.com
  - -Hijacks to a homosexual porn site
  - -Free photos of gay sexual activity

20

COFFEEBEANSUPPLY.COM

(Hijacks to a newsgroup porn site, alt.sex)

- Free Teaser Images in each Category posted at alt.sex
- Animal; stories; gay; anal; www.sex.com; oral;alt sex; sex.com; teen; pictures; gals; pics; chicks; indian; black; with animals; stories; interracial; pictures; hot; pics; lesbian; group; hardcore; asian; adult; cartoon; dog; live; phone; preteen, teenage; etc

21

WAYBACK MACHINE

- Hosted in U.S. at www.archive.org; Archives earlier versions of websites including obscenity and child pornography

Child porn
http://web.archive.org/web/*/http://Illegalhent.com
http://web.archive.org/web/*/http://Sexteen.com

Obscenity
http://web.archive.org/web/*/http://beastility.com
http://web.archive.org/web/*/http://rotten.com
http://web.archive.org/web/*/http://scatsex.com

22

YAHOO!

- Yahoo's Clubs, Members Directories and Geocities sites host child porn and encourage child sex abusers
- Yahoo! Family Incest Club
- Yahoo! Rape Club
- Yahoo! Incest Directory
- Yahoo! Child Pornography Crimes Directory

23

HARMFUL-TO-MINORS (HTM)

- 97% of adult web sites (containing obscene and/or htm content) do NOT require adult verification (Child-pornography on the World Wide Web: A Survey of Adult Webservers 2001, Internet Watch Foundation, 2003)
- Children are exposed to both online obscenity and harmful-to-minors material since the Child Online Protection Act is not in effect
- Unprosecuted obscenity meets the legal definition of harmful-to-minors.

24

Prepared by Donna Rice Hughes

10/14/03

PORNOGRAPHY- Tool used by Pedophiles

- to arouse the child
- to lower the child's inhibitions
- to demonstrate to their victims what they want them to do
- to convince the child that a particular sexual activity is okay

25

THE WORLD OF CYBERSEX

CONSUMER

26

INTERNET ACCESS (As of September 2001)

*143 million Americans (54 % of the population) have Internet access

*90 % (47.4 million) of children between the ages of 5 and 17 use computers at home or school

*75% of teens ages 14-17 use the Internet

*65% of preteens ages 10-13 use the Internet

(CNN report, Commerce Department Study, 2/7/02)

27

YOUTH AND INTERNET PORN: 2001

Among youth ages 15-17:

- 70 % have accidentally stumbled on porn online
  - "Very" or "somewhat" often (23%)
- 55% were "not too" upset
- 45% were "very" or "somewhat" upset

Of youth ages 15-24:

- 2 in 3 say being exposed to online porn could have serious impact on kids under age 18
- 59% think seeing pornography on the Internet encourages youth to have sex before they are ready

(Kaiser Family Foundation Study, 2001)

28

National Center For Missing & Exploited Children Study: 2001

Youth Access to Pornography:

- 71% searching the Internet
- 29% IM or email
- Home- 67%
- School- 15%
- Library- 3%

(NCMEC, Online Victimization: A Report on the Nation's Youth (Sample of 1,501 youth ages 10-17 who use Internet regularly, June 2001)

29

YOUTH AND INTERNET PORN: 2002

- Adult industry says some traffic is 20-30% children (NOAC Report 2002, 3.3)
- 9 in 10 kids ages 8-16 have viewed porn online, mostly unintentionally, and when using the Internet to do homework (UK, News Telegraph, NOP Research Group, 1/7/02)
  - 11-year-old girl doing homework logs into a website labeled "Adolf Hitler pictures." She is faced with child pornography, "gayexxfilepics"
  - Two brothers, aged 10 and 12, found homosexual images instead of pop band Boyzone

30

Prepared by Donna Rice Hughes

10/14/03

CYBERSEX- Crack Cocaine of Sex Addiction

- "Sex on the net is like heroin. It grabs them and takes over their lives" (Dr. Mark Sewart, Masters & Johnson, NYT, May, 2000)
- Cybersex is a public health hazard exploding because very few are recognizing it as such or taking it seriously (MSNBC/Stanford/Duquesne Study, AP 2000).
- Cybersex reinforces and normalizes sexual disorders (Dr. Robert Weiss, Sexual Recovery Institute, Washington Times, 1/26/00).

31

CYBERSEX COMPULSIONS

- 60% of all website visits are sexual in nature
- Sex is the # 1 searched word online
- 25 million Americans visit cybersex sites between 1-10 hours per week. Another 4.7 million in excess of 11 hours per week (does not include children who are becoming addicted).
- 200,000 considered "sex addicts" either lost their marriage, job, or both.
- 20 million people visit sex sites each month (MSNBC/Stanford/Duquesne Survey of 9,265 people, 2000).
- 37% of pastors say it is a current struggle (Christianity Today, Leadership Survey, 12/2001).

32

WOMEN AND CYBERSEX COMPULSIONS

- Women had slightly lower rate of sexually compulsive Internet behavior (MSNBC/Stanford/Duquesne Study, 2000).
- One out of every six women (17% of U.S. population) struggles with an addiction to pornography (Zogby International as reported in Today's Christian Woman, Sept./Oct. 2003).
- More than 80% of women who have this addiction take it offline (Today's Christian Woman, Sept./Oct. 2003).

33

STUDENTS & CYBERSEX COMPULSIONS

- Students were most at risk for cybersex compulsions
- Due to a combination of increased access to computers, more private leisure time, & developmental stage characterized by increased sexual awareness & experimentation (All stats from MSNBC/Stanford/Duquesne Study, 2000)

34

JUST HARMLESS FUN?
(Full report at enough.org)

A rope with five strands: (No Smoking Gun)

1. Advertising
2. Impact of sexually-oriented businesses
3. Controlled research studies
4. Correlational research studies
5. Experience of clinical psychologists

(+ anecdotal evidence of people whose lives have been harmed)
(Just Harmless Fun? Special Report, Enough is Enough!, 2000. Full report at enough.org)

35

1. - Advertising

- If images don't influence behavior, how do we explain the existence of the advertising industry?
- Visual images create brand images:
  - Marlboro Man, Pepsi Generation, Nike, etc.
- What brand of sexuality is pornography promoting?

(Just Harmless Fun? Special Report, Enough is Enough!, 2000. Full report at enough.org)

36

Prepared by Donna Rice Hughes

10/14/03

Overall Messages

- Advertising impacts attitudes & behavior
- Sex sells
- Pornography advertises sex:
  - Without relationship
  - Without commitment
  - Without consequences

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

37

Portrayal of Women

- "The characteristic portrayal of women in pornography [is] as socially non-discriminating, as hysterically euphoric in response to just about any sexual or pseudosexual stimulation, and as eager to accommodate seemingly any and every sexual request."

(Zillman & Bryant, 1984)

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

38

Pornography's Missing Messages

- STD's: Waiting for the results of an HIV test
- Unwanted Pregnancy: A girlfriend pregnant at 16
- A student facing prosecution for date rape because he couldn't decode the word "no"
- His partner, traumatized
- Negative impact on families and marriages

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

39

2.- Sexually-Oriented Businesses (SOB's)

- "You don't need a moral micrometer to recognize the sex industry turned Times Square into a slum."

George Will, Newsweek, 1996

- Zoning of SOBs is constitutionally permitted because of "secondary harmful effects."
  - Sexual offenses, property crimes, decrease in values
- Ever wonder what causes "secondary harm"?

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

40

3. RESEARCH STUDIES

Two types of research on pornography:

1) Controlled research – lab conditions, controlled to neutralize extraneous variables: identifies causation
2) Correlational studies – observation of real world events: identifies correlation (i.e. that certain things happen together), not causation (i.e. that one thing caused the other)

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

41

Controlled Research

- Correct test is the preponderance of the evidence
- Best approaches bring together multiple studies:
  - "review studies" (that compare the results of multi-original research studies)
  - "meta-analyses" (that aggregate original studies meeting stringent tests of comparability)

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

42

Prepared by Donna Rice Hughes

10/14/03

Example Review Study

- 1994 review study of 81 original peer-reviewed research studies:
  - "The empirical research on the effects of aggressive pornography shows, with fairly impressive consistency, that exposure to these materials has a negative effect on attitudes toward women and the perceived likelihood to rape."

(Lyons, Anderson and Larsen)

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

43

Example Meta-Analysis

- 1995 meta-analysis based on 24 original experimental studies:
  - "violence within the pornography is not necessary to increase the acceptance of rape myths"
  - which is of concern because "several recent meta-analyses demonstrate a high correlation between attitude and behavior"

(Allen, Emmers, Gebhardt & Giery)

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

44

4. Correlational Studies

- Must be used with care, since silent on causation
- ACLU asks: "Does pornography cause rape, or are rapists simply the sort of people who like pornography?"
- Why don't they ask: Does drunk driving cause accidents, or are reckless drivers simply the sort of people who like to get loaded?
- Correlation is an accepted tool as the second blade on the social science research scissors:
  - One blade for causality
  - One blade for real-world application

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

45

Examples Of Correlational Studies

- Oklahoma City: Closed 150 out of 163 SOBs in five years; reported rapes declined 27% in same period, while rising 19% in rest of state.
- Porn magazines: various studies found "strong evidence of very robust, direct correlation between circulation of sex magazines [in a state] and rape rates," even after controlling for other variables.
- Rape has increased by 500% in U.S. since 1960, parallels growth of pornography industry (Protecting Your Child in an X-rated World, Lifeway, Tyndale, 2001).

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

46

5. Clinical Psychologists

- Fortune magazine cover story, 5/15/99 - "Addicted to Sex" – described destructive effects of pornography, prostitution and promiscuity on individuals and businesses (neutral source)
- Study of 932 sex addicts, 90% of men and 77% of women said pornography played a significant role in their addiction (Patrick Carnes, whose clinic was featured in the Fortune article, 1991)

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

47

Four Stage Progression:

Dr. Victor Cline, University of Utah:

1. Addiction- The need to keep coming back for more (drug of choice).
2. Escalation- The need for more explicit, rougher & more deviant images for same effect.
3. Desensitization- Material once shocking or taboo is acceptable.
4. Acting out- Tendency to sexually act-out behaviors depicted in porn (promiscuity, bondage, rape, child molestation). Public safety issue.

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

48

Prepared by Donna Rice Hughes

10/14/03

Market Illustrates Trend

- The first three stages describe precisely the "progression" of the commercial "men's" magazine over the last thirty years:
  - Penthouse 1970 – NO full frontal nudity
  - Penthouse 2000 – oral sex, vaginal intercourse (PCV), anal penetration with object, female urination
  - 2001- Vaginal & oral sex too tame-- progression to anal sex to maintain the excitement. Writer Martin Amis did an investigative piece for The Guardian newspaper, 2001.
  - Penthouse 2001, Bob Guccione explains the growing market for a thing called bukkake ("facials" with multiple males participating).

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

49

Biological Brain Responses

Why? Imprinting

- Adrenal hormone – Epinephrine – responds to emotional stimuli by locking in memories
- Hormone- Opioids – released by nerve endings in response to pleasure – reinforce the body's desire to repeat the process (1985-James McGaugh, Phd. American Psychologist)

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

50

Factors Particularly Affecting Children

- Why are there no controlled research studies on impact of pornography on children?
  - Because they would violate ethical and professional guidelines
  - Ethical Principles of American Psychological Association require "fully informed and competent decision to participate" with risks "understood by participants"

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

51

Teenagers

- Dr. Jennings Bryant, in a study of 600 American male and female teenagers, 91% males and 82% females exposed to hard-core porn. Over 66% of males and 40% of females wanted to try out some of the sexual behaviors. 31% of males and 18% of females admitted actually doing some of the things they had seen in pornography within a few days after exposure (verse Cites, Pornography Effects).

(Just Harmless Fun? Special Report, Enough Is Enough!, 2000. Full report at enough.org)

52

Harms to Children

Edit Online: Protecting Your Children in Cyberspace, Pete Hughes 1998

- Interferes with a child's development and identity
- Shapes attitudes and Values
- Promotes Desensitization
- May incite children to act out sexually against other children
- Typical age of first exposure- 5 yrs old!

(Protecting Your Child in an Xrated World, LaRue/York Tyndale, 2002)

53

JUVENILE PERPETRATORS

- Juveniles-
  - 48% of overall solicitations
  - 48% of aggressive solicitations
- Adult solicitors-
  - Most of the "adult" solicitors were ages 18-25
  - 24% of solicitations
  - 34% of aggressive solicitations

- (NCMEC, Online Victimization: A Report on the Nation's Youth (Sample of 1,501 youth ages 10-17 who use Internet regularly, June 2001)

54

Prepared by Donna Rice Hughes

10/14/03

Child Rapists

- Nearly half of the nation's child molesters were children (Philadelphia Enquirer, 1993)
- Juvenile sex offender programs:
  - 22 in 1983
  - 755 in 1993
  - 1200 in 2002 (Protecting Your Child in an X-rated World, Lattau/York Tyndale, 2002)

55

THE SEARCH FOR SOLUTIONS

What should we do?

56

ENOUGH IS ENOUGH'S THREE- PRONG SOLUTION

PREVENTION

•A shared responsibility between the

Public- Parents, Schools, Libraries, Businesses, Churches

Technology Industry

Legal Community- Law Enforcement & Public Policy

•Each provides an essential layer of protection

57

PUBLIC PRONG

ROLE OF PARENTS, TEACHERS, & LIBRARIANS

-Awareness, education and empowerment

-Safety Rules and Software tools- Both are essential, one without the other is ineffective

-Gov't can't parent, & parents can't enforce the laws

58

Techno-Phobic and Internet Challenged Parents

- 43% of children who have visited x-rated sites said they do not have rules about Internet use at home (Time/CNN Poll, 2000)
- 62% of parents are unaware that their children had accessed objectionable sites (Yankelovich Partner Survey, 07/1999)
- 1 in 2 parents don't use protective software (Time/PC 1999)

59

PUBLIC LIBRARIES

- Public Libraries had 82 million Internet sessions- annual porn incident rate of between 400,000 and 2 million (Dangerous Access, 2000).
- 7,000 porn sites accessed in 2 days in Chesterfield, VA's 9 public libraries. Board of Supervisors voted to filter all terminals (June 2001).

60

Prepared by Donna Rice Hughes

10/14/03

TECHNOLOGY PRONG

WHAT CAN THE TECHNOLOGY INDUSTRY DO?

- Develop technological solutions
- Implement technological solutions
- Industry Code of Conduct
- Choose not to offer newsgroups offering child pornography & obscenity
- Cooperate with law enforcement

61

Toxic Environment

- How do we protect ourselves, our children, from the secondary effects in a culture that allows such toxic material to flourish?
- How do we protect our children from others who may act out violently against them because of their own exposure to pornography?

62

Acting Out

- 11/98- 11-year-old Josh had been looking at graphic violent porn on the Internet for 20 minutes immediately before stabbing 8-year-old Maddie Clifton to death.
- 6/29/98- 13-year-old (boy) was in the Phoenix Burton Barr Library viewing porn on the Internet. He followed a 4-year-old into the bathroom and asked the younger boy to give him oral sex (Dangerous Access, 2000).

63

LEGAL PRONG

GOVERNMENT & LAW ENFORCEMENT

- Aggressive enforcement of current laws (child porn, obscenity, child stalking laws)
- Federal, State, & Local cooperation & coordination
- Law enforcement training
- The public should not have to shoulder the burden of protecting against illegal content and criminal activity

64

Legislation

- Child Online Protection Act (COPA)- Adult verification required on porn sites
- Child Internet Protection Act (CIPA)- Requires Schools & Libraries to filter
- Loopholes- New Laws and Rulemaking: Spam, Deceptive Marketing Tactics, Mousetrapping

65

COPA Commission Recommendations (www.copa.org)

- Gov't at all levels should fund, with significant new money, aggressive programs to investigate, prosecute and report violations of federal and state obscenity laws, "including efforts to protect children from obscenity."
- Make available a list of Internet sources (no images) found to contain child porn and obscenity
- Pursuant to Congressional rulemaking enforcement- deceptive, unfair business practices (mousetrapping, deceptive meta-tagging, spam)

66

Prepared by Donna Rice Hughes

10/14/03

National Research Council Recommendations

- "Vigorous prosecution of obscene material"
- Civil liability
- Enforcement of record-keeping requirements
- Streamline process of handling violations
- New rulemaking (spam, mousetrapping)

67

Public Support for Enforcement

- 76% of Americans think Internet porn should be banned
- The more accessible the medium, the less permissible sexually-explicit content should be: (% allowed)

Video 37%	Basic Cable 74%
Premium Cable 41%	Internet 76%
Magazines 55%	

(Sixth of the First Amendment, 1999 Freedom Forum)

68

Wirthlin Survey, 2002

- Eight out of ten Americans (81%) believe federal laws against Internet obscenity should be vigorously enforced, and seven out of ten (70%) believe that strongly. A higher percentage of women support vigorous enforcement of federal laws against Internet obscenity than men (90% versus 72%).
- On the other hand, seven out of ten Americans (70%) say they do not believe these laws are currently being vigorously enforced.

69

Adult Internet Industry Conference (source: www.ai2000.com)

- "Peaches & cream as far as prosecutions" under the Clinton administration (Paul Cambria, Attorney to Porn Industry, CNS News, 9/24/00)
- The industry has enjoyed "benevolent neglect" under Janet Reno (Adult Video News, 1999)

70

Enough Is Enough! -Appeal to Law Enforcement

- Public opinion drives public policy
- The pornographers have and will continue to push the envelope
- Take back the ground we've lost
- Collective & coordinated united front
- Only prosecution and law enforcement can turn the tide

71

Prepared by Donna Rice Hughes

U.S. SENATOR PATRICK LEAHY

CONTACT: David Carle, 202-224-3693 VERMONT

Statement of Senator Patrick Leahy
Ranking Member, Senate Committee on the Judiciary
Hearing on "Indecent Exposure:
Oversight of DOJ's Efforts to Protect Pornography's Victims"
October 15, 2003

Today's hearing -- which is being billed as an "oversight" hearing – will focus the Committee's attention again on issues relating to the distribution of pornography. The Committee has devoted a significant amount of time to this topic, particularly as it relates to the exploitation of children, and we have become well-versed on the subject.

Just last month, the Committee held a hearing on peer-to-peer networks, which allow individuals to share files with millions of other users in relative anonymity. Witnesses testified that these networks are harboring the vilest forms of child pornography and are increasingly impervious to law enforcement scrutiny.

Earlier this year, Congress passed the PROTECT Act – which Senator Hatch and I had developed and refined over the course of several Congressional sessions. Although not perfect, the PROTECT Act was a good faith effort to provide powerful tools for prosecutors to deal with the problem of child pornography within constitutional limits in the wake of the Supreme Court's ruling on the 1996 Child Pornography Protection Act. Regrettably, House and Senate Republicans used this bipartisan legislation as a vehicle to pass controversial sentencing provisions that had nothing to do with protecting children, and, in the words of Chief Justice Rehnquist, "seriously impair the ability of courts to impose just and responsible sentences."

One of the many positive aspects of the PROTECT Act was its updating of the Victims of Child Abuse Act of 1990. That legislation requires electronic and remote computing services to report instances of child pornography to the National Center for Missing and Exploited Children, and authorizes the Center to forward this information to law enforcement. The PROTECT Act strengthened the Center's ability to report Internet-related child sexual exploitation in the distribution of child pornography, online enticement of children for sexual acts, and child prostitution.

I am pleased to welcome our witnesses from the Department of Justice, as well as representatives of local law enforcement and pornography victims. I am looking forward to their testimony. One issue I would like to hear discussed is whether the investigation and prosecution of child pornography cases could be significantly enhanced by greater participation of local and state law enforcement. They are highly experienced, and their

senator_leahy@leahy.senate.gov
http://leahy.senate.gov/

93014.236

involvement would also free up additional Department resources for pursuit of terrorism cases and other national law enforcement concerns.

I also hope the Department witness will answer outstanding questions on the Department's efforts under the Victims of Child Abuse Act, as recently amended, to stop child pornography, especially in the peer-to-peer network context. For instance, I would also like to have a discussion of the Department's position on whether these networks are subject to the pornography reporting requirements.

It has become clear that some peer-to-peer operators take the position that this statute does not apply to them. I think it is important that we have a clear understanding – and that these network operators have a clears understanding – about their obligations, and that we do all that we can under the law to prevent their networks from being conduits for child pornography and exploitation. Indeed, I have a continuing concern that the Department has not yet issued implementing regulations updating the Victims of Child Abuse Act under the PROTECT Act. The Department has yet to provide how Internet Service Providers should comply with the statute. I note that I recently sent letters to Attorney General Ashcroft on this matter, and look forward to his response.

In the meantime, it would be instructive for us if the Department representatives here today could discuss what they know about the Department position on the obligation of P2P networks to comply with this statute, and to what extent the Department is pursuing matters against these networks as a result of their failure to report instances of child pornography.

# # # # #

93014.237

Department of Justice

STATEMENT

OF

JOHN G. MALCOLM
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

INDECENT EXPOSURE: OVERSIGHT OF DOJ'S EFFORTS TO PROTECT PORNOGRAPHY'S VICTIMS

PRESENTED ON

OCTOBER 15, 2003

Testimony of John G. Malcolm
Deputy Assistant Attorney General, Criminal Division
United States Department of Justice

before the
Senate Judiciary Committee

Indecent Exposure: Oversight of DOJ's Efforts to Protect Pornography's Victims
October 15, 2003

Mr. Chairman, Mr. Ranking Member, and esteemed Members of the Committee:

My name is John Malcolm, and I am a Deputy Assistant Attorney General in the Criminal Division of the Department of Justice. Among my other duties, I supervise the Child Exploitation and Obscenity Section (CEOS) and the Computer Crime and Intellectual Property Section (CCIPS). In addition to pornographic material, which is constitutionally-protected, adult obscene material and child pornography, which are not constitutionally-protected and which are illegal, are, unfortunately, pervasive in our society. I thank the Committee for inviting me to testify about the Department of Justice's enforcement efforts against those who produce and disseminate adult obscenity and child pornography.

I. The Nature and Scope of the Problem

Let me begin by acknowledging the positive benefits of the Internet, which are too numerous and obvious to restate here. While there is no doubt that the Internet provides access to a highly diverse network of educational and cultural content, it is also responsible for the proliferation of adult and child pornography and obscene material. Indeed, offensive material that used to be largely unavailable to average citizens and children is now largely unavoidable. Far from being hidden in brown paper bags behind the counters of disreputable stores, offensive material is now readily available to anyone with an Internet connection within a matter of

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00318 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.239

minutes with a few clicks of a computer mouse, accessed oftentimes by unsuspecting children and by adults who had no intention to seek such material and no desire to view it.

Over the last several years, online pornographers have used various technological and marketing techniques designed to trick both adults and children into viewing their offensive material. One favorite trick of online pornographers is to send pornographic spam email. Another is to utilize misleading domain names or deceptive metatags (which is a piece of text hidden in the Hypertext Markup Language (HTML) used to define a web page) which can mislead search engines into returning a pornographic web page in response to an innocuous query. As a result of these deceptive metatags, searches using terms such as "toys," "water sports," "Olsen Twins," "Britney Spears," "beanie babies," "bambi," and "doggy" can lead to pornographic websites. Indeed, it has been estimated that ninety percent of children between the ages of 8 and 16 have been exposed to obscene material on the Internet. Moreover, once an unsuspecting person is on a pornographic website, online pornographers utilize other techniques such as "mousetrapping" to prevent that individual from exiting these websites and stopping the assault of offensive material.

The proliferation of this material and the desire by pornographers to differentiate themselves in a highly-competitive market have prompted pornographers to produce ever-more offensive material. In addition to child pornography, pornography depicting and glorifying bestiality, scatology, and rape are readily available and aggressively marketed.

The harmful effects of obscene material and the victims of this sordid industry are very real. The images produced promote the idea of sex without consequences, such as unwanted pregnancies or sexually-transmitted diseases. The victims, usually women, are objectified and demeaned, presented as completely non-discriminating with respect to the number or type of

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00319 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.240

sexual partners they have and as being aroused and gratified by being beaten, tortured or raped. Very few women grow up dreaming of being filmed having sex with an animal or being raped and beaten by multiple partners, and very few who see these powerful images and absorb the antisocial values they portray can remain unaffected by them. The negative, lasting impact that this has on the participants who are in these images, and on the attitudes that are formed by the predominantly-male viewers who see them, is incalculable.

The negative impact and effects of child pornography, while more readily apparent and universally-recognized, are too horrifying to think about. Images of young teenagers, prepubescent youngsters, and literally infants engaging in sex of all types with other children and adults are readily-obtainable and would make you sick to your stomach.

Because the Internet has popularized the trade in child pornography, there has been a surge in demand and a corresponding surge in production of child pornography. A recent study by the National Society for the Prevention of Cruelty to Children ("NSPCC") indicates that approximately 20,000 images of child pornography are posted on the Internet every week. We see younger and younger children depicted in these images. Indeed, the recent NSPCC study indicates that about half of new images appearing on the Internet depict children between the age of nine and twelve, and the rest are younger.

As with obscenity, the trend with respect to child pornography is towards more violent and extreme sexual acts being committed against children. We see "custom-order" child pornography where consumers request specific types and ages of children to be molested and photographed or filmed, along with specific sexual directions to the abuser. We see molesters filming their abuse real-time with webcams and broadcasting that sexual abuse live over the Internet. Because child sexual abuse tends to occur in the home or other private location by a

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00320 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.241

person close to the child, the potential for the sexual abuse to span years is great. We must never forget that each image represents the rape of a child. Each image is a tragedy and a gruesome memorial of trauma, abuse, powerlessness, and humiliation that will be with that child for the rest of his or her life.

The Internet has proven to be a useful tool for pedophiles who are able to use it to communicate with each other, trade images, and encourage each other to continue this deviant and harmful conduct. Pedophiles also use the Internet to contact unsuspecting children in chat rooms, to befriend them and engage in sexually-explicit conversations, and, ultimately, to lure them away from the safety of their homes for illicit and dangerous assignations. In so doing, pedophiles frequently use child pornography and obscene material to lower the inhibitions of their victims and to persuade them that adult-child sexual interaction is perfectly acceptable. Too often, this pernicious ploy works.

The sad reality is that, because the Internet is borderless and seamless and because the production and dissemination of objectionable material is both pervasive and international in scope, it is highly unlikely that the Department is ever going to be able to rid our country of obscene material and child pornography through prosecution alone. Active involvement by parents and teachers in the activities of children, public awareness of the "dark side" of the Internet as well as the harm caused by obscenity and child pornography, and development and deployment of protective software tools and filters are going to be necessary components of any effective strategy to combat this scourge.

Nonetheless, the Department of Justice is aware that it must do its part. Most Americans do not want their Internet-connected homes to be besieged by an avalanche of obscene material and child pornography and overwhelmingly support law enforcement efforts to protect them and

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00321 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.242

their children. Protecting women, children, and families is something that we can all agree is a vital role for government, and that is what the Department is attempting to accomplish.

2. The Department's Efforts to Combat Adult Obscenity

Attorney General Ashcroft publicly stated that "[t]he Department ... is unequivocally committed to the task of prosecuting obscenity" and that federal prosecutors should work together with CEOS to facilitate "ongoing, systemic and aggressive obscenity investigations and prosecutions." Since that time, CEOS attorneys, working with prosecutors in U.S. Attorney's Offices around the country, have created an obscenity enforcement strategy and have made tremendous progress, along a number of fronts, in combating the scourge of obscenity.

In order to aggressively and effectively combat the online distribution of obscenity, the Department created the High Tech Investigative Unit ("HTIU"). The HTIU, which has been operational since October 2002, is staffed with computer forensic experts who bring their special technological expertise to bear against internet-based child pornography and obscenity offenders, many of whom feel impervious to law enforcement because of the perceived anonymity of the Internet. Working side-by-side with CEOS Trial Attorneys and federal agents, HTIU's computer forensic specialists meet the challenge presented by the use of emerging Internet technology in the commission of child pornography and adult obscenity crimes and are poised to meet new challenges that will surely develop as technology evolves.

While not yet fully staffed, the HTIU, working in cooperation with federal law enforcement agencies, has successfully initiated and developed several cases and has a number of matters under investigation. The HTIU continues to leverage its resources in identifying and

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00322 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.243

investigating complex online cases which may otherwise escape prosecution due to the technical challenges involved.

By formal arrangement, the HTIU receives tips from the National Center for Missing and Exploited Children (NCMEC), Morality in Media (MIM), and the Federal Trade Commission (FTC) involving child pornography and obscenity offenses. The HTIU is already receiving and reviewing an average of 120 tips per month from NCMEC and MIM and has direct access to the FTC's complaint database. Many of these complaints have been referred for further investigation. The Department appreciates the efforts of these organizations, and all citizen groups which report violations of federal law, and hopes to maintain these very beneficial relationships in the future.

CEOS devised and conducted a *Federal Prosecutors Symposium on Obscenity* held at the National Advocacy Center in June 2002. The Attorney General personally addressed the audience and, via live simulcast, also addressed U.S. Attorney's Offices throughout the country. In October 2002, CEOS presented an Obscenity Training Seminar, during which it distributed a detailed obscenity case digest. A second annual Obscenity Training Seminar began today and will last the rest of the week. It is through such training of federal prosecutors and agents that the Department hopes to develop a national strategy and framework for sustained, long-term enforcement of federal obscenity laws, to complement the anti-obscenity efforts of state and local prosecutors and investigators.

I am pleased to state that the Department's efforts in this regard are starting to bear fruit. To date, during this Administration, there have been nineteen convictions involving federal obscenity statutes. Two defendants, including a former police officer, who allegedly distributed rape videos are on trial right now in federal court in Dallas, Texas. There are three other

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00323 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.244

obscenity cases that have been indicted, including large-scale distributors of allegedly obscene material, and approximately fifty federal obscenity investigations are ongoing in districts throughout the country.

Each investigation is unique and complex, rising or falling based on the facts involved. Although it is not my purpose today to announce any new targets, nor is it my purpose to immunize any purveyors of offensive material from our federal obscenity enforcement efforts, among the factors we review are the content of the material itself, the size of the distribution network, how the material is marketed and to whom it is marketed, where the targets are located, how the material is disseminated, and where the material is disseminated.

Under the Supreme Court's test for obscenity, first announced in Miller v. California, 413 U.S. 15 (1973), two of the three prongs call for the application of "contemporary community standards." Varying community standards means that a given item may be obscene in some districts but not in others. For this reason, among others, we work closely with U.S. Attorneys in different districts because they are in the best position to determine the local standards of the communities in which they live and work. I would note, however, that those who disseminate offensive material from more permissive districts into arguably less permissive districts, a matter of particular relevance to those who distribute such material via the Internet, do so at their peril. As the Supreme Court stated recently in Ashcroft v. American Civil Liberties Union, 535 U.S. 564, 583 (2002):

> If a publisher chooses to send its material into a particular community, this Court's jurisprudence teaches that it is the publisher's responsibility to abide by that community's standards. The publisher's burden does not change simply because it decides to distribute its material to every community in the Nation.

3. The Department's Efforts to Combat Child Pornography

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00324 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.245

While the Department is committed to a renewed enforcement agenda with regard to adult obscenity, and despite the obvious divergence of federal resources to combat terrorism, the Department continues to vigorously enforce child sexual exploitation laws. Indeed, according to the Executive Office of United States Attorneys, in fiscal year 2002, 1199 cases were filed involving child pornography and child exploitation statutes (a 22% increase from FY 2001).

Internet investigations often uncover large child pornography groups with hundreds and sometimes thousands of targets. The Internet affords pedophiles the ability to exchange large amounts of child pornography with large numbers of people with minimal effort. CEOS, working closely with U.S. Attorney's Offices throughout the country, is currently involved in nine significant national operations. These investigations require coordination among law enforcement agencies, including state and local Internet Crime Against Children (ICAC) Task Forces , and prosecution entities to ensure the best utilization of our limited resources. Several of these investigations have identified and rescued child victims. Although these investigations are ongoing, and some of them are international in scope, several child molesters have already been apprehended and convicted in this country

In Operation Hamlet, for instance, the Department dismantled an international ring of active child molesters. Many of these criminals were molesting their own children, as young as 14 months old, making their children available to other members of the ring, exchanging images depicting their abuse, and, in some instances, running a "live-feed" via webcam during their abuse so the other ring members could watch the abuse in real-time. Thus far, thirteen Americans have been identified as active child molesters and another fourteen have been identified as child pornography traders. Other countries experienced similar success. Of the thirteen American child molesters, all but one (who committed suicide) have been indicted

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00325 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.246

federally (with six convictions obtained thus far). The fourteen Americans identified as child pornography traders have likewise been targeted for federal charges, with several indictments already pending.

NCMEC operates two "tiplines" designed to receive complaints of child pornography on the Internet, receiving hundreds of tips each week. CEOS works closely with NCMEC to ensure that tips, which are shared with the Federal Bureau of Investigation (FBI), Bureau of Immigration and Customs Enforcement (ICE), U.S. Postal Inspection Service (USPIS), and U.S. Secret Service (USSS), as well as state and local law enforcement, are actively pursued. Additionally, acting in coordination with other law enforcement agencies and NCMEC, CEOS devised and is currently implementing the National Child Victim Identification Program. Its mission is to gather and analyze intelligence in order to find and save children who are being sexually abused. Images of child pornography are tracked in the "database," which is able to identify images representing fresh instances of abuse. Those images, along with any intelligence data, are forwarded to law enforcement for priority investigation.

Through passage of the PROTECT Act, Congress, with the assistance of this Committee, recently provided the Department of Justice with some significant new tools to assist law enforcement in combating child pornography and thwarting child exploitation. Among its many useful provisions, the PROTECT Act requires lifetime supervised release for convicted sex offenders, creates a rebuttable presumption against pretrial release for child rapists/abductors, and eliminates the statute of limitations for child sex crimes. In addition, the Act improves existing sex tourism laws to target sex tourists and sex tour operators, limits the bases upon which sentencing judges can downwardly depart in child sex cases, and creates a "Two Strikes, You're Out" law for child sex offenders. The Truth in Domain Names provision, part of the PROTECT Act, criminalizes the use of misleading domain names to attract persons, and particularly children, to pornographic web sites.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00326 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.247

The Department is already making effective use of these tools, as evidenced by the recent indictments under the PROTECT Act (1) by the United States Attorney's Office for the Southern District of New York of John Zuccarini, who is alleged to have created and used over 3,000 misleading domain names on the Internet with the intent to deceive minors into viewing pornographic web sites, (2) by the United States Attorney's Office for the Western District of Washington of Michael Lewis Clark, who is alleged to have traveled to Cambodia to engage in sexual activity with underaged boys, and (3) by the United States Attorney's Office for the District of South Carolina of Joseph Bledsoe for possession and distribution of child pornography as that term is defined in the Act.

4. Some of the Challenges We Face

As I have discussed in some detail already, the Department faces many challenges in enforcing federal child pornography and obscenity laws. Many of these challenges relate to the complexity of investigating Internet crimes. Although the Department has made great progress in developing the technological expertise necessary to successfully investigate Internet cases, such cases can pose significant difficulties even when law enforcement has the necessary technical expertise. For example, it is often difficult to obtain records from Internet Service Providers (ISPs) which can assist law enforcement officials. There are literally thousands of ISPs, and each has a different policy regarding record retention. Some keep detailed records for long periods of time, usually to meet their own security needs, while others do not keep detailed records or retain them only for short periods.

Several of the statutes that we utilize have come under constitutional attack, which could significantly affect our ability to pursue obscenity violations and protect children from sexual exploitation. One such statute is the Child Online Protection Act (COPA) (codified at 47 U.S.C. § 231),

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00327 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.248

which was enacted by Congress in 1998 to protect children on the Internet from obscene content and content that is "harmful to minors." COPA was Congress' second attempt at protecting children from harmful content on the Internet. The first attempt, the Communications Decency Act, was struck down as unconstitutional by the Supreme Court. As of today, there is an injunction barring the Department's enforcement of the challenged COPA provisions, and the Department is seeking the Supreme Court's review of the Third Circuit's decision striking down the statute. Another lawsuit challenges the use of the traditional Miller obscenity standard in Internet cases, alleging that applying local community standards to Internet content (which has no boundaries) renders the statute unconstitutionally overbroad. See Barbara Nitke, et al. v. Ashcroft, 01 Civ. 11476 (S.D.N.Y. Dec. 14, 2001).

Conclusion

While we are addressing these challenges, we are under no illusion that they will be easy to overcome or that we will not face additional challenges in the future, particularly as new technologies emerge. Nonetheless, despite these and future challenges, the Department of Justice will do everything within its power to curb the proliferation of obscene material in our society and protect children both at home and abroad from the predatory activities of pedophiles.

I would like to thank you again for inviting me to testify on behalf of the Criminal Division of the Department of Justice, and I look forward to answering your questions.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00328 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.249

STATEMENT OF INSPECTOR IN CHARGE LAWRENCE E. MAXWELL OF THE UNITED STATES POSTAL INSPECTION SERVICE

Before the

United States Senate

Committee on the Judiciary

Hearing on "Indecent Exposure: Oversight of the Department of Justice's Efforts to Protect Pornography's Victims"

October 15, 2003

Good afternoon Mr. Chairman and members of the Judiciary Committee. I am Lawrence Maxwell, Inspector in Charge for the Fraud and Dangerous Mail Investigative programs of the U.S. Postal Inspection Service. My management responsibilities include the oversight of our child exploitation and obscenity investigations and programs. Thank you for holding this hearing on the topic of pornography and its effect on victims and society, and in particular, our children. It is an honor to appear before you today to discuss the important role of the Postal Inspection Service, both past and present, in combating obscenity and child pornography through the mail.

The U.S. Postal Inspection Service

As one of our country's oldest federal law enforcement agencies, founded by Benjamin Franklin, the United States Postal Inspection Service has a long, proud and successful history of fighting criminals who attack our nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public. For over 250 years, Postal Inspectors and our predecessors have investigated criminal offenses. From embezzlements in the colonial post offices to mail train robberies in the 1800s, from the major fraud cases in the 1900s to the mailing of deadly anthrax in 2001, Postal Inspectors have worked diligently to ensure America's confidence in the mail.

Postal Inspectors tenaciously investigate any criminal offense involving the mail or postal systems. We carry firearms, make arrests, execute federal search warrants, and serve subpoenas. In carrying out our mission, Postal Inspectors work closely with the Department of Justice and all United States Attorneys offices; other federal and local law enforcement agencies; and local prosecutors to investigate cases and prepare them for court. To effectively enforce over 200 federal laws covering investigations of crimes that adversely affect or fraudulently use the U.S.

93014.250

mail and postal system, there are approximately 1,900 Postal Inspectors stationed throughout the United States, Puerto Rico, Guam, the U.S. Virgin Islands, and Germany, as well as at Interpol Headquarters in Lyon, France, and at Universal Postal Union Headquarters in Berne, Switzerland.

History of Postal Inspectors and Obscenity Investigations

Postal Inspectors have investigated obscenity offenses for well over a century. In the 1860s and 70s, Post Office Special Agents, as Postal Inspectors were called then, had to deal with European smut peddlers who were invading American shores with obscene material. In 1873, Congress passed a law banning the use of the mail to distribute obscene material. This legislation was known as the Comstock Act, named for Post Office Inspector Anthony Comstock, who drafted the bill and urged its passage. It was a forerunner to the current postal obscenity statute (Title 18, United States Code, Section 1461).

The Postal Inspection Service investigates any criminal offense involving the mail, including violent crimes, theft, fraud, narcotics trafficking, mail bombs, money laundering, and even terrorism. We are also responsible for protecting employees, postal assets, and the public. Because we must address such broad responsibilities with limited personnel resources, there are only about 50 Postal Inspectors nationally who specialize in child exploitation and obscenity investigations. Despite this relatively small number of investigators, our success in this area has been significant.

Child Exploitation and Obscenity Investigations

While over the years child pornography offenses were, as a matter or course, investigated along with other obscenity matters, increased public concern over this material resulted in the United States Congress enacting the Sexual Exploitation of Children Act in 1977 (Title 18, U.S. Code, Section 2251-2253). This was the first federal law specifically designed to protect children from "commercialized" sexual exploitation. It was the culmination of years of effort by Congress, the Department of Justice, concerned members of the public and the law enforcement community to take action against the pernicious effects of pornography and the sexual exploitation of children.

In support of the new legislation, the U.S. Postal Inspection Service was the first federal law enforcement agency to begin aggressively identifying, targeting and arresting commercial child pornography distributors. The mail was a preferred means to traffic in this illicit material because of the security, reliability and anonymity it can provide. Use of undercover operations that were designed to ferret out these mail-order child pornography dealers proved to be most effective, and offenders were arrested and convicted under the new federal laws. During the course of conducting investigations into the commercial sale of child pornography, Postal Inspectors began encountering and arresting more and more actual child molesters—those producing the illegal material—along with their child victims.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00330 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.251

On May 21, 1984, six years after the enactment of the first federal child pornography statutes, President Ronald Reagan signed into law the Child Protection Act of 1984. This 1984 Act amended the original Act and created some new statutes, putting more "teeth" into the federal anti-child pornography laws. This Act recognized that any person trafficking in child pornography, not only people selling child pornography for profit, should be brought to justice.

In 1985, President Reagan called upon Attorney General Edwin Meese to create a panel to examine the effects of pornography, and child pornography in particular, on American society. The Commission on Pornography, as it was known, comprised a chairman and ten members. The Commission had several full-time staff investigators, one of whom was Postal Inspector Daniel Mihalko. Inspector Mihalko currently serves as the Inspector in Charge of Congressional and Public Affairs at our National Headquarters. Today, most of the recommendations made by the Attorney General's Commission on Pornography back in 1986 have been put into place. Over the past 17 years, since the Commission concluded its work, Congress has continually passed new legislation to better protect our children and close all possible loopholes in existing laws. Speaking on behalf of all the men and women of the Postal Inspection Service, we thank you for all that you and other members of Congress have done to make our world a safer place for kids.

In 1986, the Postal Inspection Service took advantage of the new laws and worked in concert with the Department of Justice to launch a proactive undercover operation, targeting for investigation persons across the country suspected of trafficking in child pornography. This nationally-coordinated investigation was known as *Project Looking Glass.* A total of 235 search warrants were obtained and served throughout the country, resulting in the arrest and conviction of 165 child pornographers, many of whom were found to be molesting children.

In 1987, the Department of Justice asked the Postal Inspection Service to take a leading role in the enforcement of federal obscenity law, specifically to investigate large mail-order companies distributing obscene materials in violation of federal statutes. Many of the companies investigated routinely mailed unwanted sexually-oriented advertisements into the homes of citizens, generating a public outcry for action. The operation was known as *Project Post Porn* and ultimately led to 50 indictments and convictions in 20 federal judicial districts. Over $5.2 million in fines were levied by the courts.

Following on the success of *Project Post Porn*, the Postal Inspection Service was again asked in 1991, by then Assistant Attorney General Robert Mueller, to conduct another series of obscenity investigations. This investigative operation was launched in 1992 and was known as *Project Mail Porn*. Although a number of obscenity dealers were convicted, the success of *Project Mail Porn* did not equal that of the earlier *Project Post Porn*. Due to a change in the priorities of federal prosecutors as a result of an Administration change, many of the cases being investigated were never charged.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00331 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.252

In 1996, Postal Inspectors dismantled a $500,000 a year mail-order child pornography enterprise. The San Diego based company, Overseas Male, was the largest commercial child pornography business known at that time. After putting the company out of business and arresting the principals, Postal Inspectors again worked with the Department of Justice's Child Exploitation and Obscenity Section to design and implement a proactive undercover operation targeting some of the more egregious violators and customers of Overseas Male. The operation was dubbed *Project Special Delivery*, and in the end, over 135 search warrants were obtained and served and more than 100 individuals were arrested and convicted. Again, many of the people identified through this child pornography investigation were also child molesters.

Recognizing a need to factually demonstrate the correlation between child pornographers and child molesters, the Postal Inspection Service began compiling statistical information from our case work in 1997. Hard data has confirmed what we, as investigators, intuitively knew: there is a direct correlation between traffickers of child pornography and child molesters. In fact, our data has revealed that at least one in three suspects arrested for child pornography offenses by Postal Inspectors has also sexually abused children. Since 1997, 757 child victims have been identified and rescued from further abuse as the result of Postal Inspectors' investigations. That is why such crimes continue to be one of our top investigative priorities.

Child Exploitation and the Internet

Use of the mail to traffic in child pornography, or otherwise sexually exploit children, continues to be a significant problem in our society. But nothing has aided the spread of child pornography as much as Internet communications. More and more child molesters and pornographers have become computer-literate and have turned to cyberspace to seek out potential victims, communicate with like-minded individuals, and locate sources of child pornography. Over the last several years, there has been a dramatic increase in the number of unlawful computer transmissions and ads for child pornography on the Internet that occur hand-in-hand with trafficking of child pornography videotapes and computer media through the mail.

In 1997, 33 percent of child exploitation cases investigated by Postal Inspectors also involved computers. Now, approximately 70 percent all of our child exploitation cases involve electronic communication in addition to postal violations. The instant file-sharing, e-mails, peer-to-peer networks, newsgroup postings, and aggressive marketing by child pornographers have made the trafficking of this material easy, quick, and virtually anonymous.

Perhaps, no other single child exploitation case has been as successful as the investigation of Landslide Productions, a company that was located in Ft. Worth, Texas. The investigation led by Postal Inspectors began in 1999. It was known as *Operation Avalanche* and was worked in partnership with the Dallas Police Department's Internet Crimes Against Children (ICAC) Task Force. Our

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00332 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.253

investigation unraveled and shutdown a multi-million dollar web-based child pornography business. In one month alone, the company grossed in excess of $1.4 million through subscription sales to child pornography websites. Again, throughout this investigation, trial attorneys from the Child Exploitation and Obscenity Section of the Department of Justice provided legal advice and guidance, working hand-in-hand with Postal Inspectors and ICAC Task Force representatives as the case expanded. Landslide's principal owner, Thomas Reedy, received an unprecedented 180-year sentence in federal prison. Nearly 200 spin-off investigations were initiated here in the United States and over 4,000 searches have now been carried out in other countries, making this the largest global action ever undertaken against child pornographers.

In another chilling case, last year, Postal Inspectors arrested an Ecuadorian national in Miami Beach, Florida, for using a commercial mail receiving agency address to sell child pornography videotapes and DVDs to customers throughout the United States. Our investigation determined the suspect produced the child pornography that he sold, sexually abusing well over 175 minor females. Tragically, this suspect is HIV positive. He remains in federal custody and is scheduled for trial later this year.

In an effort to educate the American public and reduce the incidence of child sexual abuse and exploitation, the Postal Inspection Service partnered with the National Center for Missing and Exploited Children (NCMEC) in a national crime prevention initiative designed to raise the public's awareness about the online victimization of children. This initiative centered on a simple, yet powerful, poster that was created and distributed for display in each of the 38,000 postal facilities nationwide. The poster presents the results of this first scientifically based national research studying the risks faced by children on the Internet and provides an easy reporting mechanism for such incidents through the NCMEC's Cyber Tipline.

Since the enactment of the Federal Child Protection Act of 1984, Postal Inspectors have conducted investigations resulting in the arrests of more than 4,000 child molesters and pornographers. The Postal Inspection Service is committed to this work and we remain steadfast in our determination to identify, investigate, and bring to justice those individuals who sexually abuse and exploit children.

In recognition of our work to combat the sexual exploitation of children, Postal Inspectors have been recipients of the prestigious National Missing and Exploited Children's Awards in each of the last five years for their exemplary investigations. In three of those years, Postal Inspectors have been named Officer of the Year. No other agency has achieved such acclaim. The awards are presented during a Congressional Breakfast and Awards Ceremony here on Capitol Hill each May.

Adult Obscenity Investigations

In addition to targeting the producers and consumers of child pornography, we also investigate commercial distributors of materials that violate the federal obscenity laws. Our efforts in these most recent investigations mirror the prosecutive climate

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00333 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.254

of the respective federal judicial districts. Our obscenity investigations are conducted in total partnership with the Child Exploitation and Obscenity Section (CEOS) of the Department of Justice and with the individual United States Attorneys offices where the cases are charged.

In the past, obscene materials involving the actions of consenting adults had to be specifically sought out by the people that wanted them, and there were typically some efforts to restrict access by minors. As Internet use has become commonplace, the purveyors of these materials have begun to aggressively market their products. It is difficult to maneuver through the Internet, or even maintain an e-mail account, without being bombarded by offers of the most graphic, vile, and obscene sexual materials. Flashing banner advertisements, spam e-mails, and a creative variety of other marketing methods invite any Internet user to the pornographic and obscene products. The websites boldly offer images of teen and pre-teen sex; individuals engaging in sexual activity with animals (bestiality); brutal sexual violence including rape and genital mutilation; and, sexualized behavior involving defecation and urination. Unfortunately, much of this purchased material, videotapes, and DVDs is distributed via the U.S. Mail, in violation of federal law.

Today, the offers are not limited to those adults who specifically seek them—they are virtually unavoidable for any Internet user, including children. Numerous pornographers have intentionally acquired seemingly harmless Internet domain names that are especially likely to invite children. They have also acquired domain addresses similar to popular mainstream websites in an intentional effort to snare individuals who mistype Internet addresses.

Earlier this year, Congress enacted and the President signed into law the Truth in Domain Names Act, under the PROTECT Act, which made it illegal to knowingly use a misleading domain name on the Internet with the intent to deceive a person into viewing material constituting obscenity, and a crime to knowingly use a misleading domain name with the intent to deceive a minor into viewing "material that is harmful to minors" on the Internet.

In the very first federal prosecution under this new law, originating in the Southern District of New York (SDNY), one notorious Internet operator, John Zuccarini stands accused of registering at least 3,000 Internet domain names that included misspellings and slight variations of popular names like "DisneyLand," "Nsync", "Teletubbies," "Britney Spears," "Bob the Builder," and "Yahoo." Zuccarini earned up to a million dollars per year from leasing these domain names to pornographers. Inadvertent typing mistakes by children and others with no intent of accessing Internet pornography led directly to obscene materials. The Federal Trade Commission received numerous complaints from consumers who had unintentionally accessed websites controlled by this individual and were suddenly barraged by pornographic materials through a practice commonly referred to as "mousetrapping." Attempts to exit the websites often opened additional pornographic websites, and many users had to shut down their computers to escape the onslaught of sexually-graphic material. The FTC began civil actions, and requested the assistance of the Postal Inspection Service to pursue a criminal

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00334 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.255

investigation. We did, in cooperation with United States Attorney James Comey (SDNY), and we arrested the defendant in his hotel room in Florida last month.

The tactics currently used by obscenity dealers are so outrageous that they appear to operate under an assumption of impunity and social acceptance. We believe the community disagrees, and the recent prosecutions and jury convictions support our investigative priorities. Since so many of the businesses use the mail to distribute videotapes, printed materials, and computer media, we have not, and will not, hesitate to pursue investigations that lead to criminal prosecution of individuals and companies violating federal obscenity law.

A few of our recent investigations are summarized below.

- A trial is set to begin this month for a former Dallas, Texas, police officer and his wife on charges stemming from the mailing of obscene matter. The couple owned, managed and maintained a website named "The Rape Video Store," where they offered obscene video tapes depicting rape scenes, which they categorized on the website as the "Real Rape Video Series" and the "Brutally Raped Video Series." This case was investigated jointly by Postal Inspectors and the Federal Bureau of Investigation (FBI). As with other obscenity investigations, we pursued this investigation in a much-valued partnership with the Department of Justice Child Exploitation Obscenity Section (DOJ-CEOS).
- On August 6, a ten-count federal indictment was returned against Extreme Associates of North Hollywood, California, and its owners, at Pittsburgh, Pennsylvania, following a seven-month investigation conducted by Postal Inspectors and detectives of the Los Angeles Police Department. The charges result from the company's distribution of obscene videotapes and DVDs depicting rape and violent sexual abuse to individuals through the mail and to wholesale distributors throughout the United States. The videotapes and DVDs included titles such as, "Forced Entry—Director's Cut" and "Extreme Teen #24." This case is also a result of our partnership with the DOJ-CEOS, and is being prosecuted by the office of Western District of Pennsylvania United States Attorney Mary Beth Buchanan.
- Four individuals pled guilty to federal obscenity charges on August 25 in Beckley, West Virginia. The investigation by Postal Inspectors, working with the Department of Justice, Child Exploitation and Obscenity Section, determined their company, using an Internet website, conducted business from Lewisburg, West Virginia and Quitman, Georgia. The company distributed video tapes and DVDs by mail that depicted graphic and sexually explicit scenes of defecation and urination. Visitors to the website now find the official seals of the Postal Inspection Service and the Department of Justice, with this message displayed as notice and warning: "The website formerly known as 'www.girlspooping.com' has been forfeited to the United States Government pursuant to the prosecution of the website's owners and operators for violations of federal obscenity laws, including mailing obscene matters and conspiracy to use the Internet for

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00335 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.256

the purpose of sale and distribution of obscene material, pursuant to 18 United States Code Sections 1461 and 371."

- In 2000, Postal Inspectors investigated a Florida company known as New Technology that was responsible for mailing out particularly offensive videos depicting males and females engaging in sex acts with dogs, horses, goats, and eels. They also advertised and sold an assortment of rape re-enactment videos. New Technology purchased large mailing lists and sent unsolicited advertisements to citizens all across the country. A United States Magistrate Judge in Houston received one of these solicitations, and immediately contacted Postal Inspectors. Following an undercover investigation, Postal Inspectors executed a search warrant on the offices of New Technologies and seized videotapes, computers, and business records. In the ten months preceding the search, the business made more than a million dollars in sales for their bestiality videos. Guilty pleas for mailing obscene materials were obtained from the two owners of the business and their company.

- The owner of an Internet website, Taboomovies.net, was successfully prosecuted in the Eastern District of Kentucky (EDKY) last December following and investigation into the distribution by mail of obscene videotapes. The videotapes that were sold depicted rape scenes, bestiality, and extreme physical and sexual abuse, including the mutilation of women's genitals. The investigation was carried out by Postal Inspectors and prosecuted by the U.S. Attorney's office for the EDKY, in cooperation with the CEOS/DOJ. The individual was recently sentenced to six months in prison and ordered to pay a $2,500 fine. The defendant received a downward departure from the sentencing guidelines due to his significant cooperation with the government that has led to a number of new investigations.

Currently, we have ongoing obscenity investigations being conducted in a number of states, from coast to coast, and more federal prosecutions can be expected. You can also be certain that the Postal Inspection Service will continue to work with all other federal, state, and local law enforcement agencies, and the Department of Justice to aggressively investigate, arrest, and seek prosecution of those individuals who use the mails to traffic in child pornography and obscene materials.

Senator Hatch, the U.S. Postal Inspection Service applauds your support of the law enforcement community in this fight.

I would be happy to answer any questions that you have at this time.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00336 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.257

Testimony of Detective Steven Takeshita (LAPD) before the Senate Judiciary Committee on the "Indecent Exposure: Oversight of DOJ's Efforts to Protect Pornography's Victims"

Good afternoon honorable ladies and gentlemen of the Senate Judiciary Committee. I am Detective Steven Takeshita and I am the Officer-In-Charge of the Pornography Unit at the Organized Crime and Vice Division of the Los Angeles Police Department.

Before I begin, I would like to thank the Honorable Committee for their invitation to provide, which I hope, will be useful testimony about the pornography industry. I am a twenty-five year veteran of the department and I have been investigating the distribution of obscenity for the past eighteen years. I have developed my expertise over the years by working with more experienced officers and by obtaining first hand experience as the undercover operative in a joint investigation with the Federal Bureau of Investigation (FBI) into the nationwide distribution of obscenity.

In the 1950's, the Los Angeles Police Department formed the Pornography Unit when it became aware that the pornography industry was developing its base in the Los Angeles area. The duties of the unit were to monitor the distribution of pornographic material and to prosecute the illegal distribution of obscenity as it affected the quality of life to the citizens of Los Angeles.

During this time period the adult industry was taking advantage of the resources available in the Los Angeles area for their productions. The hopeful actors and actresses and the support personnel were all willing to participate in the industry to meet their basic financial obligations. Because of the wide variety of

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00337 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.259

scenic locations and great weather both the general and adult film industries favored the Los Angeles area. They could film a mountain, desert or beach scene, all in one day, an ideal environment for filming.

The industry has progressed from the "TJ Bibles" (sexually explicit pocketbooks bought in Tijuana) and 8mm films to the DVD and Internet. The Internet has been referred to as the Wild West of the 90's. This Wild West of the 90's has progressed to the point where the average distributor on the Internet, thinks that they are immune from prosecution because of the Internet. The Internet is just a vehicle for distribution. For example, if I were telephoning a minor to entice the minor for sexual activity there would not be a difference than if I chatted on line for the sexual activity with the same minor. It is just a vehicle for the illegal activity.

This vehicle has posed new investigative methods. No longer do we respond to an advertisement in the local adult periodical to find the distributor in our backyard. Now our response maybe directed to a city across the nation or even to a foreign country. Since our investigations deal directly with a person's First Amendment Rights, all of our investigative evidence is acquired with either a Search Warrant or a consent search. No longer can we establish agency liaisons only within our own county, but now we need to network with agencies across the nation and sometimes worldwide. These liaisons are critical for our surveillances and Search Warrant endorsements.

The Los Angeles area is no longer the base of distribution for 90% of the adult product within our nation, as it was in the earlier years. The increased use of the Internet has made the distribution of obscenity a national problem. The extreme adult product distributed now days was self-banned by the adult industry at large only ten years ago. The recent lax in federal and local prosecution

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00338 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.260

of obscenity has brought forth the courage in the adult industry to produce this extreme sexually explicit product. The adult industry must produce different types of products to encourage the consumer to continue in the purchasing of their product. The tight competition for the consumer dollar has encouraged the major adult industry producers to venture to the edge of the envelope with the distribution of some of the most extreme sexual product.

We have the laws in place to protect the abuse the women endure during the filming of these extreme sexual videos. We have the laws in place to protect the exposure of this type of product to our children. We have the laws in place to create a better quality of life for our citizens. We need the assistance of the federal government to prosecute the violators of the statues that Congress have enacted to put the welfare of our communities as one of our priorities.

Most recently, the Western District of Pennsylvania, United States Attorney Mary Beth Buchanan and her staff, the Child Exploitation and Obscenity Section (CEOS) of the United States Department of Justice and the United States Postal Inspection Service have investigated and also provided assistance to our investigations into the distribution of obscenity. These entities have been very supportive and taken the lead into investigating the distribution of obscenity.

What we need to do today is for all law enforcement agencies to prosecute aggressively any violator of the distribution of obscenity within their investigative jurisdiction to the maximum penalty.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00339 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.261

The First Amendment is listed first, because our Forefathers felt its importance. The adult industry tries to hide behind the First Amendment in the distribution of their product. The Supreme Court has ruled that the First Amendment does not protect obscenity.

Thank you honorable ladies and gentlemen of the Senate Judiciary Committee for providing me this opportunity to testify before you.

VerDate Aug 31 2005 14:03 Jul 17, 2008 Jkt 093014 PO 00000 Frm 00340 Fmt 6601 Sfmt 6601 S:\GPO\HEARINGS\93014.TXT SJUD1 PsN: CMORC

93014.262

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

HEARING OF OCTOBER 15, 2003,
"INDECENT EXPOSURE: OVERSIGHT OF DOJ'S EFFORTS TO PROTECT PORNOGRAPHY'S VICTIMS"

STATEMENT OF BRUCE A. TAYLOR
PRESIDENT AND CHIEF COUNSEL
NATIONAL LAW CENTER FOR CHILDREN AND FAMILIES

3819 PLAZA DRIVE, FAIRFAX, VA 22030
(703) 691-4626, FAX: -4669
WWW.NATIONALLAWCENTER.ORG
BRUCETAYLOR@NATIONALLAWCENTER.ORG

93014.263

Mr. Chairman and Members of the Committee:

Obscenity is a crime and deserves to be prosecuted to the fullest extent of the law. It has been an offense to traffic in obscenity since the beginning of our Nation and is still a crime under Federal law and the laws of nearly every State. Because it is a crime and because organized crime has always played a dangerous role in controlling the porn syndicates that make and distribute hard-core pornography, I believe obscenity should be treated as any other serious crime and prosecuted in persistent and fair fashion, consistent with the Equal Protection Clause that should insure that all violators share an equal chance at facing justice in the courts of law. I also agree with the Congress and the State Legislatures that obscenity and its modern extreme form known as child pornography are not victimless crimes and contribute to anti-social conduct, sex crimes, deterioration of neighborhoods, and influence attitudes and activities among men, women, and children that contribute to a lack of respect for human dignity, personal privacy, mutual rights, and personal safety.[1] As the Supreme Court said in the *Paris Adult Theatre* case in 1973, "The sum of experience...affords an ample basis for legislatures to conclude that a sensitive, key relationship of human existence, central to family life, community welfare, and the development of human personality, can be debased and distorted by crass commercial exploitation of sex. ... The States [and Congress] have the power to make a morally neutral judgment that public exhibition of obscene material, or commerce in such material, has a tendency to injure the community as a whole, to endanger the public safety, or to jeopardize, in Mr. Chief Justice Warren's words, the States' 'right...to maintain a decent society'."[2]

I have been prosecuting obscenity cases for thirty years, since June 21, 1973, when the Supreme Court handed down the famous *Miller* decisions and gave us a three-prong test to separate illegal pornography from expression protected by the First Amendment. I was a law clerk in the Cleveland Prosecutor's Office and was asked that day by the Chief Prosecutor to read the new opinions and see how they would change how that office prosecuted its obscenity cases. Over the next five years, I would handle over 600 obscenity cases, obtain over 450 guilty pleas, and see jury convictions in all but two of at least 38 obscenity jury trials in Cleveland Municipal Court. Between 1976 and 1981, we would also prevail in over 100 obscenity law appeals, including before the Supreme Court of Ohio, the U.S. Court of Appeals for the Sixth Circuit, and the Supreme Court of the United States. The Cleveland Police brought cases against all known employees of all the hard-core obscenity outlets and against all types of the hard-core pornography sold and the City's prosecutors brought those cases into the courts. Because of my having learned this field of prosecution under a policy of full and fair law enforcement, I have continued to prosecute and assist in the prosecution of obscenity, child exploitation, prostitution, and related vice crimes as both a special prosecutor for counties and cities across the Country and as a federal prosecutor for DOJ's Child Exploitation and Obscenity Section from 1989 through 1994. I have now been in about 100 jury trials for such offenses in almost half of the States. I have been in state and federal courts in big cities like Los Angeles, Phoenix, Cleveland,

---

[1] In several cases over the past three decades, the Supreme Court and other state and federal courts have recognized the harmful secondary effects of sexually oriented businesses that specialize in pornography and commercial nudity and upheld the right of cities and counties to enact zoning and licensing ordinances based on reports and studies of their destructive impact. There are at least forty studies and reports of municipalities and state agencies that have documented such crime impacts and urban blight, including those reports from such diverse communities as Los Angeles, Cleveland, New York City, Phoenix, Minneapolis, Indianapolis, Seattle, Oklahoma City, Houston, Dallas, El Paso, Las Vegas, Alliance, Ohio, Newport News, Virginia, Manatee County, Florida, Adams County, Colorado, and New Hanover County, North Carolina.

[2] *Paris Adult Theatre I v. Slaton*, 413 U.S. 49, at 63, 69 (1973).

Cincinnati, Las Vegas, Houston, Miami, and Indianapolis, and in smaller communities such as Fort Wayne, Jeffersonville, Concord, Horry County, South Carolina, and Brazos County, Texas. On occasion, some of those obscenity or child porn cases involved extreme forms of what used to be "underground" materials, such as ABCDE porn (Animals, Bondage, Children, Deviance, Excretory), but almost all of the cases I had the privilege to act as a state or federal government attorney have involved hard-core pornography depicting adults engaged in explicit sexual conduct with "PCV" (penetration clearly visible). This is the "hard-core pornography" that the "porn syndicates" produce by pimping performers into actual sex acts for money in violation of state prostitution laws (and often the Federal "Mann Act," 18 U.S.C. § 2421, *et seq.*, for interstate travel for prostitution purposes). It is this PCV form of hard-core pornography that has always been recognized as within the legitimate scope of Federal and State obscenity laws and prosecutable by prosecutors in any and every jurisdiction in the United States. The porn industry knows the line well and has, until recently, kept it to itself. Hollywood has never crossed that line and only the porn syndicate members and their associates have dared to occupy that territory. It is an objective line that allows prosecution policy to be consistent and predictable across urban and rural borders and known to the offenders and juries alike. In fact, I suggested in a law review article that Congress and the States could consider adopting a *per se* law to prohibit traffic in "hard-core pornography" that shows penetration clearly visible and lacks serious literary, artistic, political, or scientific value or purpose.[3] In light of the rampant and technologically sophisticated nature of today's Internet and wireless transmissions of hard-core obscenity within, into, and out of the United States, it is worth considering whether such a *per se* obscenity law for hard-core pornography would be an effective and constitutionally permissible law enforcement measure for Congress to enact to deter this crime in this modern age.

We applaud the renewed efforts of the Department of Justice to begin again to enforce Federal obscenity statutes against this criminal activity and we will continue to encourage the Criminal Division's Child Exploitation and Obscenity Section to take on the challenge and privilege of enforcing these laws against the unlawful traffic in obscenity over the Internet, over the airways, in America's cities, and at our borders.[4] The Attorney General has repeatedly stated his intent and policy of full enforcement of Federal obscenity laws, as well as increased enforcement of child exploitation and trafficking laws, both in his public addresses and in his policy statements to the Department and the United States Attorneys. His word must not be allowed to fail and their recent efforts must be continued "to the fullest extent of the law." It has taken some time for the Department to re-staff CEOS, train the new federal prosecutors, and begin co-training with U.S. Attorneys offices and federal law enforcement investigators at the U.S. Postal Inspection Service and FBI. The first federal obscenity cases in a decade have been indicted this year. These efforts must be continued and supported so that this crime may be successfully prosecuted for the benefit of the next generation of our children, grand-children, spouses, families, and victims. The specialized First Amendment sensitive and industry specific training and experience sharing must continue among federal and state prosecutors and police agencies. Federal resources should be strengthened by funding and implementing the 25 additional

---

[3] Taylor, Bruce, University of Michigan Journal of Law Reform, *"Hard-Core Pornography: A Proposal for a Per Se Rule"*, 21 U. Mich. J.L. Ref. 255-82 (1988).

[4] As noted by the Supreme Court in *Roth v. United States*, 354 U.S. 476, at 485 n. 15 (1957), and *New York v. Ferber*, 458 U.S. 747, at 754 (1982), there is an international Treaty that can be used by U.S. and other Nations to cooperate in identifying and prosecuting obscenity offenses. The original Treaty is called "Agreement for the Suppression of the Circulation of Obscene Publications", signed at Paris, May 4, 1910. In the U.S., it is reported at 37 Stat. Pt. 2, p. 1511, Treaties in Force 209 (U.S. Dept. of State), Treaty Series 559. The 1949 Protocol transferred the recording and tracking functions to the United Nations. There are now over 130 signatory countries.

prosecutors that Congress provided for CEOS as part of the PROTECT Act of 2003 to handle obscenity and child exploitation cases. Federal and State efforts could also be dramatically increased by regular appointment of local assistant district attorneys and county prosecutors as cross-designated special assistant United States Attorneys to work on federal felony obscenity cases in the Federal courts, to complement or take the place of state law prosecutions (that are sometimes felonies, for wholesale promotion or repeat offenses, but often misdemeanors for retail traffic or first offenders). Joint obscenity and child exploitation, and trafficking seminars should be regularly held in regional locations across the Country to facilitate knowledgeable, consistent, and constitutionally sound investigations and prosecutions on both Federal and State levels. This is a national and international crime that is committed primarily by a syndicate of hard-core pornographers who supply the obscenity to local porn shops, commercial Websites, video outlets, and pay-per-view movie services. Effective and fair enforcement of Federal and State laws requires the latest information and the highest standards of law enforcement to deal with this complex and widespread criminal enterprise. Existing laws can be effective, if universally enforced and the public deserves the benefit of those laws and deserves the continued vigilance of the Congress in keeping our laws up to date and in seeing that they are well and justly enforced against those who knowingly pander unprotected pornography in violation of those existing and future laws.

There are three classes of unprotected pornography that Congress and the States have prohibited from commercial and public distribution under criminal statutes, nuisance abatement statutes, and civil injunction laws, which are Obscenity, Child Pornography, and Harmful To Minors pornography.

Obscenity (which may include all hard-core adult pornography) is not protected by the First Amendment and is unlawful to produce or sell under the laws of most States and is a felony under Federal laws to transmit or transport by any facility of interstate or foreign commerce.

Obscene pornography is unprotected even for "consenting adults" and the Supreme Court upheld the right of Congress to declare it contraband and prohibit the use of any means or facility of interstate or foreign commerce to move or ship any obscene materials. Under existing U.S. Code sections, traffic in obscenity is a felony offense, such as 18 U.S.C. § 1461 (crime to knowingly mail obscenity, even for private use, or to mail advertisements for obscenity), § 1462 (crime to knowingly import/export or ship obscenity by common carrier via ground, air, water, satellite, Internet, phone, TV, or cable, etc., even for private use), § 1465 (crime to knowingly transport obscenity, for sale or distribution, across state lines or by any means or facility of interstate or foreign commerce, §§ 2252 & 2252A (crime to knowingly transport, receive, or possess child pornography within, into, or out of the United States by any means, including computer, and § 1961, *et seq.*, RICO crime for knowingly using an enterprise in a pattern of obscenity or child exploitation offenses (including federal and state violations).

The Supreme Court has consistently held that obscenity is not protected speech under the Constitution and upheld the power of Congress and State Legislatures to prohibit obscenity from the streams of commerce. "This much has been categorically settled by the Court, that obscene material is unprotected by the First Amendment." *Miller v. California*, 413 U.S. 15, at 23 (1973). This is true even for "consenting adults." *Paris Adult Theatre v. Slaton*, 413 U.S. 49, at 57-59 (1973). "Transmitting obscenity and child pornography, whether via the Internet or other means, is already illegal under federal law for both adults and juveniles." *Reno v. ACLU*, 521 U.S. 844, 117 S.Ct. 2329, at 2347, n. 44 (1997). The "*Miller* Test" was announced by the Court to provide

the legal guidelines for determining obscenity under both federal and state laws. *See Miller v. California*, 413 U.S. 15, at 24-25 (1973); *Smith v. United States*, 431 U.S. 291, at 300-02, 309 (1977); *Pope v. Illinois*, 481 U.S. 497, at 500-01 (1987), providing the three-prong constitutional criteria for federal and state law enforcement and court adjudications:

(1) whether the average person, applying contemporary adult community standards, would find that the material, taken as a whole, appeals to a prurient interest in sex (*i.e.*, an erotic, lascivious, abnormal, unhealthy, degrading, shameful, or morbid interest in nudity, sex, or excretion); and
(2) whether the average person, applying contemporary adult community standards, would find that the work depicts or describes, in a patently offensive way, sexual conduct (*i.e.*, "ultimate sexual acts, normal or perverted, actual or simulated; ... masturbation, excretory functions, and lewd exhibition of the genitals"; and sadomasochistic sexual abuse); and
(3) whether a reasonable person would find that the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Child Pornography consists of an unprotected visual depiction of a minor child under age 18 engaged in actual or simulated sexual conduct, including a lewd or lascivious exhibition of the genitals. It is a crime under Federal and State laws to knowingly make, send, receive, or possess child pornography. *See* 18 U.S.C. § 2256 and 2256A; *New York v. Ferber*, 458 U.S. 747 (1982), *Osborne v. Ohio*, 495 U.S. 103 (1990), *United States v. X-Citement Video, Inc.*, 115 S.Ct. 464 (1994). *See also United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987), *United States v. Knox*, 32 F.3d 733 (3rd Cir. 1994), *cert. denied*, 115 S. Ct. 897 (1995). In 1996, 18 U.S.C. § 2252A was enacted to include "child pornography" that consists of a visual depiction that "is or appears to be" of an actual minor engaging in "sexually explicit conduct". Section 2252A was upheld as Congress intended it to apply to computer generated realistic images that cannot be distinguished from actual photos of real children in *United States v. Hilton*, 167 F.3d 61 (1st Cir. 1999), and *United States v. Acheson*, 195 F.3d 645 (11th Cir. 1999), but the Supreme Court declared the statute invalid as applied to child pornography that is wholly generated by means of computer in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002). Congress then amended that law in the PROTECT Act of 2003, S.151, which also enacted a new section 18 U.S.C. § 1466A to give greater penalty for obscene child pornography.

Pornography Harmful To Minors (which may include soft-core pornography) is unlawful to knowingly sell or display to minor children under State laws and under federal law as enacted in the Child Online Protection Act of 1998 (COPA, 47 U.S.C. § 230), even if the material is not obscene or unlawful for adults. "HTM/OFM" pornography is known as "variable obscenity" or what is "obscene for minors". *See Ginsberg v. New York,* 390 U.S. 629 (1968), as modified by *Miller, Smith, Pope, supra. See also Commonwealth v. American Booksellers Ass'n*, 372 S.E.2d 618 (Va. 1988), *followed, American Booksellers Ass'n v. Commonwealth of Va.*, 882 F.2d 125 (4th Cir. 1989), *Crawford v. Lungren*, 96 F.3d 380 (9th Cir. 1996), *cert. denied*, 117 S. Ct. 1249 (1997). Under the "*Miller*ized-*Ginsberg* Test," pornography is "Harmful To Minors" or "Obscene For Minors" when it meets the following three prong test, as defined by statute and properly construed by the courts and judged in reference to the age group of minors in the intended and probable recipient audience:

(1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion (as judged by the average person, applying contemporary adult community standards with respect to what prurient appeal it would have for minors in the intended and probable recipient age group of minors); and

(2) depicts or describes, in a patently offensive way with respect to what is suitable for 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 (as judged by the average person, applying contemporary adult community standards with respect to what would be patently offensive for minors in the intended and probable recipient age group of minors); and
(3) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors (as judged by a reasonable person with respect to what would have serious value as to minors in the age groups of the intended and probable recipient audience of minors).

In addition to criminalizing traffic in obscenity and child pornography for both adults and minors, Congress has acted to provide further provisions to protect children from exposure to adult and child pornography, starting with COPA in 1998 to stop commercial porn Websites from showing free teaser samples of pornographic pictures on their front pages and to require an adult identifier such as a PIN or credit card number to exclude minors. Congress also required federally subsidized schools and libraries to use Internet filters to attempt to restrict adult access to visual images of Obscenity (hard-core pornography) and Child Pornography (sexually explicit images of minors) and to also try to block pornography that is Harmful To Minors ("Obscene For Minors") on terminals while used by minors under 17, as part of the Children's Internet Protection Act of 2000, recently upheld in *United States v. American Library Ass'n*, 529 U.S. ___, 123 S.Ct. 2297 (2003). Finally, as part of the PROTECT Act of 2003, Congress amended the Communications Decency Act of 1996 in light of the Court's 1997 decision in *Reno v. ACLU*, and thereby re-instituted 47 U.S.C. § 223 to require Internet sites and providers to take good faith steps to prevent the knowing display to minors of obscenity or child pornography.

It cannot be said that Congress has not given law enforcement the tools to protect the public from the harms of illegal pornography and the intent is clear to continue to maintain and improve those laws for the good of society and the protection of victims of pornography. It is essential to preserving respect for the laws of public morality and to do as the Supreme Court recognized as the "right of the Nation and of the States to maintain a decent society", as well as to protect the next generation of children, women, and men from the harms and addiction of pornography, that these laws be persistently and consistently enforced against all classes of offenders who violate our laws and against all classes of unprotected pornography that are prohibited by those laws, by the prosecutors and police who are charged with the duty and privilege to enforce these Federal and State laws for the good of all our children and families.

Respectfully submitted,
Bruce A. Taylor
President & Chief Counsel
National Law Center for Children and Families