TESTIMONY OF DETECTIVE LEANNE SHIREY ON THE MARKETING OF SEXUALLY EXPLICIT MATERIAL

COPA COMMISSION HEARING III
AUGUST 3-4, 2000
SAN JOSE STATE UNIVERSITY

CONTACT INFORMATION:

DETECTIVE LEANNE SHIREY
C/O SEATTLE PD VICE SECTION
1519 12TH AVENUE
SEATTLE, WA 98122
(206) 684-8651
LeShirey@aol.com

TESTIMONY OF DETECTIVE LEANNE SHIREY ON
THE MARKETING OF SEXUALLY EXPLICIT MATERIAL

COPA COMMISSION HEARING III
AUGUST 3-4, 2000
SAN JOSE STATE UNIVERSITY

Mr. Chairman and members of the commission, thank you for the opportunity to be here today to discuss the marketing of sexually explicit materials online and what can be done to enhance efforts to protect children in cyberspace.

A recently released survey of 5000 youths, conducted for the National Center for Missing and Exploited Children, reports that in the past year, 25% of adolescents and teens received unwanted exposure to sexually explicit material and one in five, who regularly socialize on the Internet, encountered a stranger who wanted cybersex. 75% ignored the advances; the remaining 25% did not.

The assumption may be that kids want access to everything online – in some cases this is true – but in most cases, kids neither want, nor are emotionally capable of having, access to all content. Many of them think they are invincible, not recognizing the dangers that adults, with more life experience, understand.

Recently, I asked a group of middle school and high school students the following question: If there was one law you could make for the Internet, what would it be? They answered that there should be less advertisements and pornography, and more efforts to make the Internet safer for children. This particular group was very clear about what they want and they are looking to all of us to help them achieve it. Unfortunately, the problems associated with the Internet are going to get much worse before they get better, because the medium is growing faster than our ability to educate and empower those responsible for safeguarding our children.

Marketing sexually explicit materials

When we consider the marketing of sexually explicit materials on the Internet, we have to keep in mind that the Internet allows anyone to easily market this content. Unlike broadcast and print, which take a "one to many" marketing approach, the Internet by virtue of its decentralized design, allows a "many-to-many" approach. If we couple this with the fact that much of the adult content available on the Internet today is constitutionally protected and lucrative not only for the adult industry, but for many of the companies that are gateways to the online world, we are faced with the fact that this material, for better or worse, is here to stay. Kids stumble into adult content through innocent Internet searches, because many adult sites use misleading meta tags to drive more traffic to their sites. They can also be held hostage by an endless loop of pornography that traps them in a sea of shocking images with no easy exit.

Email is another popular conduit for marketing sexually explicit material. Marketers troll the Internet looking for online profiles with email addresses and typically share them with other marketers. They also tend to use innocuous-looking subject lines or personalized clichés to lure unsuspecting targets into opening them. Out of natural curiosity, children often click the link in the message, and if they continue to be curious, they can borrow or steal credit card to enter sites for people over 18, or create their own credit card using one of many different credit-card generating programs available on the Internet. Many Web sites owners with visitor-driven revenue models could care less who clicks on their sites, how old they are, or whether they are interested in pornographic material. Their goal, in most cases, is to capture visitors' eyes and tap into their bank accounts.

Instant messaging systems, which are extremely popular among children, are another common vehicle for purveyors of pornography. Similar to email, unsuspecting users are often sent a cleverly disguised link in a text message that leads directly to adult sites or even child pornography. Pedophiles often use this material to introduce children to sexually oriented activities and prime them for further exploitation. Pornography is a regular player in most of my Internet investigations regarding the sexual exploitation of children online.

Technological Solutions

Once the scope of the problem is accurately identified and effectively communicated, it follows that those who have a legitimate interest in protecting children online will seek out ways to fulfill this goal. Children need guidance in the virtual world, just as they do in the physical world and caregivers need assistance.

While technology tools come in many different forms and have some limitations, they are a helpful addition to any strategy for managing children's online access. Tools that allow parents to decide which content is appropriate, when that content should be accessed and how personal information is shared, helps them maintain more awareness and take action if necessary to teach their children how to be responsible online.

Software tools carry a negative connotation in some circles and are often referred to by opponents as "censorware." The term censorship can mean several different things, but if a parent is attempting to prevent her 5-year-old from viewing age inappropriate materials, or her 13-year-old from the potential of being sexually exploited by a pedophile, is it not her right to do so in her own home and under her own terms? It is virtually guaranteed that if a child uses chat and instant messaging, has full access to the Web and other online areas, he is going to see sexually explicit material and be approached by strangers, at one time or another. Software can never take the place of an involved parent, but it can be a useful ally.

The biggest drawback for parents, who want to use software tools to shield their children from inappropriate content, is the fact that the overwhelming majority of software tools don't filter content within instant messenger services. Some monitoring tools are available, but they don't prevent these materials from being viewed, and only provide notification after content is sent or received. The challenges facing filtering software are based mainly on interoperability problems. Companies marketing instant messaging services, and any other Internet program, should be encouraged to join forces to make sure that there are workable solutions for all online areas. Finding common ground in the interest of child safety and consumer confidence in the Internet should drive all responsible online companies. Sharing information would allow corporations that market filtering and blocking software tools to write code that is compatible with instant

messenger services and allow parents and others to block or filter content for children *before* they are exposed to it.

Education

There is one absolutely essential component of protecting children online and that is educating the *adult* population about the Internet and encouraging them to get involved in what their children are doing online. We made, and are still making, a large mistake where the Internet is concerned. Knowing that the Internet is a large part of our children's future we have focused most of our educational efforts on them. We have largely left the adults out of the picture. We should have gotten all of the good adults on the Internet first, then brought the children on board. The adults are the mentors, educators, and watch keepers of our nation's youth. Instead, we turned America's children loose on the Internet without giving their parents and caregivers the tools and knowledge they needed to supervise them.

No other technology in our history can compare. Even something as simple as using the telephone requires parental guidance and rules, as well as a level of comfort with the technology that gives them the means to supervise their children. The Internet is infinitely more powerful than a telephone, yet we allow children to use it for hours at a time, largely without rules, safeguards, safety training, or parental supervision. This does not make common sense. How can we expect parents to raise their kids in the digital age if they don't understand the environment to which their children are being exposed? One of the biggest challenges facing adults is that the cyber world is moving so fast. As one parent told me, there is never a time that a parent can catch his breath and get up to speed with this technology. It causes a panic and a feeling of helplessness.

Protection Through Partnership

Perhaps the most heartbreaking part of my job as an investigator of Internet crime and the sexual molestation of children is to hear from parents that if they had just known ahead of time what their children were getting into, they would have done something to prevent it. Hearing this lament time after time, prompted me to seek out a network of like-minded volunteers to create a hands-on, non-threatening educational program for caregivers, law enforcement, and others.

Following our belief in *Protection through Partnership*, "The Internet and Your Child" organization promotes a networked, coordinated response from all levels of law enforcement, partnered with computer security specialists, corporations, such as Net Nanny and Microsoft, organizations such as the Washington State Internet Service Providers, and educators from across the United States. The program is soon to be expanded outside of our country's borders. This breaking down of the bright lines of our traditional roles and jurisdictional borders is mandated by the very nature of the Internet's design. To become effective in the prevention and reaction to cyber crime and related issues we must similarly adapt and work together toward a common goal of increased understanding and user empowerment.

People have the best chance to manage Internet use if we give them the information they need to make informed decisions for themselves, their families and their communities. When they understand the issues, establish rules, and use tools to help them enforce those rules, they will have much more confidence in the Internet. They will feel less overwhelmed by the Internet crime stories they hear and read in the news. They will know that their children can be protected while using the Internet and that they have a person that they can call for assistance if necessary. I am encouraged that this grassroots partnership expands daily and that more people are benefiting from greater knowledge, but like any other grassroots program, we wish we had more people and resources to meet demand.

Cooperation Among Law Enforcement

The Internet is changing the way all of us communicate and law enforcement must change and adapt to the way we handle crime on the Internet. Law enforcement at every level needs to share in the responsibility of policing the Internet, because it is not uncommon for a victim to be in one state and the suspect to be in another. It is not practical to assume that the federal government and federal law enforcement agencies can handle all of the crime on the Internet any more than we would expect them to be able to handle all of the drug problems in this country.

There are promising examples of law enforcement working together across jurisdictional boundaries to bring successful arrests and prosecutions of those using the Internet for illegal purposes. The decentralization of the Internet has made this necessary and the efforts to network

and rise above traditional jurisdictional politics are making this successful. Working together, separate jurisdictions can create bring a positive conclusion to the prosecution of these criminals.

Seattle's Internet Crimes Against Children task force is one of 30 task forces formed across the United States to prosecute crime and educate communities about protecting children against sexual exploitation. I am proud that my department is committed to serve as an encouraging example of the effectiveness of multi-jurisdictional cooperation across all levels of law enforcement.

Statistics

Frequently, I am asked for statistics related to crime on the Internet. Currently, there are only a select number of law enforcement agencies that report Internet crime statistics to a central location. The vast majority of agencies across the U.S. have no effective means of collecting and tracking Internet-related statistics and accurately assessing the need for resources.

While the FBI's Innocent Images task force reports a 1200% increase in tips related to Internet crimes against children and child pornography, this increase is due in part to recent reporting by 30 new Internet Crimes Against Children task forces. Formed over the past two years through grants from the Office of Juvenile Justice and Delinquency Prevention, these task forces are required to report all of their criminal cases and cyber tips to Innocent Images. But because other law enforcement agencies do not contribute to this central reporting, we do not know how many cases and cyber tips are being investigated in addition to the FBI, US Customs, and the 30 previously mentioned ICAC task forces.

While municipal, county, and state law enforcement agencies send crime statistics to the FBI as part of the Uniformed Crime Reporting, they have no means of specifying cases that have an Internet component. A rape of a child involving a next-door neighbor is counted in the same category as one involving a person who lured a child via the Internet. One solution would be to add a marker for crimes containing an Internet component, so that law enforcement can easily include these as part of the statistics they send to the FBI. This would give statistic seekers a better basis of determining the scope of the problem across *all* law enforcement jurisdictions.

With more accurate statistics, policymakers and voters would have the information they need to assess crime trends, prioritize legislation, meet the demand for additional educational programs and increase crime-fighting resources.

Tools for Prosecutors

While law enforcement needs more resources to fight cyber crime, we cannot leave out our crucial partner - the judicial system. Because of the decentralized nature of the Internet, suspects or witnesses are often located in different parts of the country. Local prosecutors are willing to bring charges against a suspect, but often they don't have the budgets to enable witnesses and victims to testify in the jurisdiction in which the crime took place. One proposed solution is to set aside funds, perhaps under the auspices of the National Association of Attorneys General, to help local prosecutors obtain this necessary testimony. They could also use additional funding to hire technology-related expert witnesses when the need arises. This funding would help law enforcement prosecute more crimes, providing an effective deterrent to those who seek to put our nation's children in harm's way.

Tools for Investigators

I recently spoke with an Oregon FBI agent who was involved in preventing a school shooting. In that case a young Oregon teen received an email from her Internet pen pal, who told her he intended to go to his school the next day and shoot some students. The Oregon teen notified her father, who in turn notified the local rural county law enforcement agency. The police on the West Coast received the initial report at 11 pm. The assigned county investigator had worked with the Hillsboro, Oregon High Tech Crime task force on an unrelated matter a few years earlier and called them for assistance. Members of that task force were reached and the investigators, including the Oregon FBI agent, who was part of this task force, worked through the night to identify the person who had sent the email, and ended up preventing the threat from being carried out. The FBI agent told me that all involved were working against the clock and had difficulty locating contact information for the security personnel of the specific Internet service providers, often calling numbers that only had automated voicemail systems. The agent said that the originating County law enforcement agency did not even own a computer scanner to convert evidentiary documents to electronic form so they could be forwarded to the assisting

investigators. The County agency had to get help from a local business, which opened their office so they could use their equipment. Eventually, they were able to trace the email to a student in Virginia, a location 3 hours later than the West Coast. Two hours before school started, the involved law enforcement agencies were able to identify the student and place him under surveillance at his home, while school officials were contacted and a search of the school property and students' locker were done for weapons. As the student left for school he was taken into custody. Officers found a hunting knife and shotgun shells on his person and a shotgun in his bedroom. All involved are convinced that this student did indeed intend to shoot students at school that day.

While this is a wonderful example of networking and effectively working together across multiple jurisdictional lines, it also points out some common problems for investigators. Lack of equipment is a constant hindrance for most law enforcement jurisdictions. Over 90% of this country's law enforcement agencies have fewer than 50 officers. With the Internet requiring all law enforcement agencies to become a cyber crime-fighting partner, we must do more to make sure they have the necessary equipment and training to do their jobs effectively. Time, in many instances, is of the essence. The FBI agent said he worked from home using his own equipment, because there wasn't even enough time to drive to his office. He said that all involved were slowed down in their investigative efforts to identify the suspect because of difficulty in locating ISP security contact information and personnel during the night. This case points out the fact that often Internet investigations of all types require response from law enforcement at a time when business offices are normally closed. Investigations that mandate a rapid response are significantly slowed as the officer spends time on the telephone attempting to reach a correct number for an ISPs security employee.

One simple solution would be to have a central database, accessible around the clock to law enforcement and other system security professionals, of all ISPs and their 24-hour security contact information. From my own experience, I would also recommend that this database include telephone company contact information and listings of phone prefixes with their attendant companies. Currently, if a telephone company leases part of their lines to a secondary provider, the law enforcement investigator cannot get the secondary company's identity without

sending a subpoena to the parent phone company. It is time consuming and frustrating to then receive back a response to the subpoena that the second telephone company holds the requested telephone number subscriber information and that obtaining their name and address requires a second subpoena submission. Learning which telephone or pager company has control of which telephone numbers should be as simple for investigators as requesting it by telephone.

Industry Regulation

The groups who create and market sexually explicit material must accept a significant level of responsibility to shield children from this material. While many adult content providers are responsible, many are not. It is either going to take effective self-regulation or a mandate by government to improve the present situation.

The adult industry should police itself or be mandated to only use meta tags that are directly related to their site content. If an ISP finds them in violation of this requirement, the ISP may remove them from their site and report the violation to the Federal Trade Commission. A simple "truth-in-advertising" requirement should apply on the Internet, just as it does offline. This would help prevent "accidental viewing" by unsuspecting children and adults of sites not related to the keyword search they were doing.

The rest of the adult community should strive to match their progressive competitors and rate their sites based on their content as well as submit their sites to child safety software vendors. Adult sites should also consider mirroring their physical world counterparts, who wrap their magazines in a protective cover to shield young eyes. Installing privacy screens that cover genitalia and other controversial imagery on their teaser pages would help protect children's sensibilities if they happen to stumble onto adult-oriented sites, either by mistake or by design.

Conclusion

We live in a culture of 30-second sound bites, which set an expectation that people can and should learn about Internet issues in an instant. Those of us who regularly work within this medium know that there are no quick answers and no easy solutions. Many people have unrealistic expectations that cause them to believe that there should be one magic tool or a set of

laws that will take care of the problem of objectionable material because they don't understand the Internet's complexities. These are not only the caregivers of our children; they are also voters whom we ask to support Internet legislation. They are also the jurors who are called to decide the guilt or innocence of anyone charged under the criminal statutes that we are working in good faith to pass and enforce. The graphic and violent images being marketed on the Internet today are a far cry from the soft porn magazines that adults sneaked a peak of when they were young. We cannot expect people to effectively guide children in the digital world if they don't have a clear understanding of what the issues are and what they can do to help make children's experiences safe and positive. We all have an obligation to help those less informed make good decisions about their kids' online activities.

Thank you.