Testimony Of Detective Michael Sullivan

With the limited time and resources available to law enforcement today, it is imperative that whatever actions or assistance comes from new laws or guidelines for the Internet, those actions must have the greatest impact in the area that most negatively affects our children. Since nineteen ninety four the Naperville Illinois Police Department's Computer Crimes Unit has been involved in more than five hundred computer crime investigations. The vast majority of those investigations have involved crimes of child exploitation and molestation. The alarming growth in reported crimes involving child exploitation is not specific to Illinois, the Midwest or even the United States. The growth of crime in this area is best shown in the statistics gathered by the Federal Bureau of Investigation's, Operation Innocent Images, where for the past two reporting years they have shown a twelve hundred percent increase in computer related child exploitation crime.

The bulk of the child exploitation takes place in the form of child pornography or sexual solicitation of a child. In the six years that the Naperville Police Department, and the Illinois Attorney Generals' Child Exploitation Task Force have investigated these types of crime, we have found that more than ninety five percent have involved attempted physical contact between the child and the predators. . The most dangerous areas of the Internet for children are chatrooms and one on one messaging ie. Instant Messenger. Most cases we have investigated involve the use of a chatroom and instant messaging system or "whisper" mode. This format allows the offender to search out their victim in a "virtual park", selecting their age, sex and geographical location. After observing the chat conversations of their potential victim the predator checks the profile for background information. This is the basic information needed to approach the child. The next, more serious, approaches are made in an instant message and E-mail format.
On-line child predators come from every walk of life. We have arrested businessmen, managers, ministers, schoolteachers and members of every branch of the military. In one case we had a schoolteacher drive twenty-two hours From Texas to Chicago to molest a high school freshman. In another case a man drove eighteen hours through a blinding snowstorm to get to his 12-year-old male victim. After being apprehended the pedophile admitted to sexually molesting 35 other children. And still in another case the child's parents discovered the online contact with the predator and they terminated the online account. However, the parents did not know that the relationship online had already become sexual in nature. The child, now convinced that the predator was a better friend then her parents, continued the online contact via computers at her school. In this case the predator made arrangements to meet the child at her school. The predator met the child in the school parking lot and molested her on school grounds.
Typically we have seen the following types of behaviors during the luring process:
The predators will build trust by asking the child to perform simple tasks that help the predator confirm that they are speaking with a child such as requesting a telephone call from the child to hear the child's voice. The predators will continue with sexual requests such as; sexually posed images or nude images. The child can use a digital camera or scanner to send photos via e-mail and if they do not have access to these devices they will

send photos via the mail. Unfortunately, a child in search of a friend, will agree to these requests, and are easily coerced into committing sexual acts. Most important they commit acts of deception to prevent parents from finding out about the relationship. Generally, the approach by instant messaging is not observed or documented by parents, ISPs or filtering technology. However sites such as FREEZONE.COM use live adult supervision to monitor chatroom behavior and do report attempted violation of law to the police. Other products monitor chat rooms, and bar the potential predator from the chatroom for flagrant or obvious solicitations, and still other products allow the parent to turn Chat and instant messaging off so it is not available to the child. . However this is not the norm in most on-line services, and the attempted sexual solicitation of the child is never documented or reported. The predator is sent, undocumented back to the chatrooms in another area, to look for another unknowing, and unprotected victim.

To better understand why documenting such actions is vital, you must realize that if you allow your child to go online unprotected, they will see sexually explicit content, they will be spoken to in a profane nature and they will be speaking with sexual predator. That is one hundred percent guaranteed.

Unfortunately, all to often we are called in to assist in the investigation after a child has been molested. We join the local Police Department's investigator at the hospital and try to explain how the child was approached online. Then, what can be done to locate the predator, secure the necessary evidence to arrest and convict the predator. As the facts surrounding the meeting between their child and the predator unfold they find out that this predator has molested other children in other areas of the country, and that his chats, even though were monitored, those attempts were never reported. The activities of the predator were never documented or given to anyone in an attempt to stop the abuse. Instead, the predator was free to continue roaming the Internet searching for other children to molest.

I believe existing technology, properly applied, will prevent an on-line predator from establishing a relationship with a child. The predator can be stopped months before a "real world" meeting could be arranged.

I know from my work that there are several very important issues concerning blocking, filtering or censoring any content on the Internet. But looking beyond that, the issue of child exploitation especially regarding child predators should have the highest priority. Software to enable parents and educators must be one based on content and not address blocking and must be able to scan all facets of a child's computer activity. This especially includes chat, whisper modes, browsers, e-mail and attachments. Content that is sexually explicit, harassing, predatory or even death threats can be filtered and kept away from children.

We have found two products that can monitor in all of these areas and provide law enforcement with sufficient information to take further action against an on-line predator. They are Cyber Sentinel and Predator Guard. The anti-predator libraries included in these products were developed in conjunction with multiple on-line predator investigations and are very effective. Predator Guard is interesting because it can be used on top of any other filtering solution. It is used strictly for the detection of Child Predators and provides an important layer of protection. The most critical part of this software is that it takes a screen capture of the prohibited material and stores it in a

secured database, that only the parents have access to. They can view the violation, and determine if law enforcement needs to be informed and then discuss the violation with their child. Parents are able to supervise their children's on-line activities without standing over the computer. I believe the most successful way to help protect our children is to empower parents with awareness and simple, effective software that allows the parents to detect a problem **before** it reaches my desk.
Thank You for the opportunity to testify.
Detective Michael Sullivan