TESTIMONY OF DAN JUDE
PRESIDENT
SECURITY SOFTWARE SYSTEMS INC.
Before the
COPA COMMISSION
AUGUST 04,2000
SAN JOSE, CA.

Mr. Chairman, Honorable Commissioners thank you for this opportunity to testify before your Commission. My name is Dan Jude and I am the President of Security Software Systems. Our company provides computer software solutions designed to protect children from on-line pornography and on-line predators. Our products are very effective yet not restrictive. The mission of our company is to provide a safe on-line environment for children.

Congress has a responsibility to draft legislation that will not restrict on-line free speech principles, yet protect children from accessing Web based material intended for an adult audience. This is a challenging task.

The Internet has experienced an incredible growth rate of almost 100% per year since 1988. Content is being added at a rate of 7 million pages a day with 2.1 billion pages already available on-line. This explosive growth and popularity has made the Internet an indispensable vehicle for information, communication and

commerce. With such a vast interactive audience, a wide diversity of content is available to the average Internet user. Unrestricted access provides the ultimate diversity in thought, information, culture, art, music and sex.

Sexually explicit material is a large, diverse part of the Internet. Thousands of explicit web sites exist with millions of pages of very explicit material. But sexually explicit sites are only a portion of the Child Protection problem. Working with Law Enforcement, we learned that a real danger for children lies in E-mail, Chat rooms, and Instant messaging. The Internet has provided a "virtual" playground for sexual predators and pedophiles. A typical scenario for a predator is to survey chat rooms to find a lonely or shunned child and profile them. Then move to private messaging or e-mail to cement a stronger bond. Then, after repeated contacts a "real world" meeting is generally arranged which results in the child being molested.

We studied the problem and concluded a more dynamic solution was needed. A solution capable of monitoring any form of chat, instant message or e-mail.

When I was growing up, mom always told me "don't talk to strangers". When a child is in a chat room, the room is full of strangers. The Internet provides a

form of anonymity that provides opportunity for people to say and do things they probably would not face-to-face. It also provides an almost endless supply of those types of opportunities. For adults, these "high risk" areas are more a matter of personal choice, but for children the danger is real.

Because of the real-time nature of the Internet, the speed of information transfer is only limited by the connection. Personal communications have evolved from basic BBS to Chat to Instant Messaging systems that provide one-on-one private communication. Current statistics point to 180 million users of Instant Messaging products worldwide. This new forum provides opportunities for private personal messages that benefit the majority of users. The down side is individuals with devious intentions also use this forum. On-line child predators use technology to their advantage.

In early 1997, after a year of testing and refining, we developed a new child protection application "Cyber Sentinel". It proved to be exceptional at detecting explicit web based material and was unique because of its total reliance on a content model. Part of the technology developed was the ability to gather all the text being transferred to and from the computer, including hidden or non-visible text. We then included functionality to provide different

monitoring modes, provisions for users to put in personal information and most importantly the ability to capture and store visual records of "violations".

The next major milestone in our development to provide a safe on-line environment for children was the development of our Predator Library. Many Internet related criminal investigations relate directly to predators contacting children in chat rooms, instant messages and e-mail. Chat rooms are very popular with children and are a widely used part of the on-line experience. Working with law enforcement, we reviewed hundreds of hours of recorded illicit Chat, and together developed our predator library, which recognizes and identifies words, phrases and other jargon used by online predators and pedophiles. If detected, the conversation will be recorded and stored for review by an adult and can be used by law enforcement as evidence. The application can also be configured to issue a warning to the child or immediately terminate the conversation. We've also built-in a feature that can automatically e-mail an adult if a violation has occurred.

Client-side content monitoring has advantages over other solutions. Its greatest asset is the ability to scan incoming content in "real-time". If information is inappropriate the screen can be covered and if the tool is

sophisticated enough, a data history is maintained for adult review. Bringing an adult into the process is critical for any technology to be effective.

There are many excellent filtering and blocking products available, but none offer real-time protection for children in chat rooms, instant messaging, e-mail and e-mail attachments. To complete the protection circle we developed "Predator Guard". Predator Guard was designed to work as a stand-alone application or in tandem with existing filtering and blocking technology to enhance them into a full child protection solution. Predator Guard monitors all incoming and outgoing messages, and when the conversation fits the profile of a predator or pedophile, Predator Guard takes control. A capture database provides a visual record of violations for review by an adult, or which law enforcement can use to pursue a predator.

Another monitoring approach we have taken is Policy Central. For organizations that do not block or filter the Internet or for organizations who want to reinforce their use policy, we developed Policy Central. This software application reinforces acceptable use policy when a user attempts to "login" or enter specific applications. Upon entering an application, the user must accept the

terms of the policy before they can proceed. This new approach also provides content monitoring capabilities to assure policies are being observed.

Security Software Systems is concentrating it's developmental efforts in monitoring technology and making it available to satisfy a wide array of requirements schools, libraries, business, Government and parents demand for their specific needs. Whether it is simply reminding users of an acceptable use policy or expressly denying access to sexually explicit or highly vulgar material, solutions exist that are inexpensive, versatile and effective if properly implemented.

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

Thank you for this opportunity to testify