Testimony of Gordon Ross, President and CEO
Net Nanny Software International, Inc.

COPA Commission Hearing
"Filtering and Labeling"

University of Richmond
Richmond, VA
June 20, 2000

15831 NE 8th, Suite 200, Bellevue, WA 98008
Phone: (425) 688-3008, Fax: (425) 688-3010

Introduction

I appreciate the opportunity to be here today before the COPA Commission to discuss client-side filtering technologies. Few technologies have been given as much attention, generated such controversy and caused so much confusion. This is largely due to conflicting views about how they *actually* work versus how people *think* they work. One thing is certain – according to the Annenburg Public Policy Center, three-quarters of parents in the U.S. are concerned about what their kids are doing online and want to do something about it. There is clearly a need for filtering technology. Why is it that only one-third has chosen to use them?

Some argue that consumers don't think filters are necessary while others argue that consumers don't know enough about online dangers to recognize the need for filters. Still others claim that consumers are paralyzed by mixed messages. And it's no wonder. On one hand, filters are supported as effective alternatives to Internet legislation and, on the other, they are dismissed, as ineffective tools that threaten our right to free speech – at different times these opinions have even come from the same source! Given this discrepancy, it understandable why filters have been slow to gain widespread adoption.

The goals of protecting children online and promoting the unfettered growth of the Internet are both noble, but often they are seen as mutually exclusive. Each side cancels out the other's argument, offering equally compelling evidence to support its point. It's time to focus our energies, which is why I am encouraged that the COPA Commission and others are committed to addressing both concerns. I am pleased to have the opportunity today to help increase understanding and build cooperation among these interested parties.

What is a client-side filter?

A client-side filter, like Net Nanny and others, is a software program that is installed on an individual computer, giving the parent varying degrees of control over how and when Internet content is used. Not all client-side filters work exactly the same way, though there is the tendency to lump them together. Each company has its own business and product models, its own way of building enhancements and maintaining databases. Each company markets its product differently and has a distinct philosophy.

The one thing we do have in common is that we provide tools to control children's online activities. Generally, client-side filters work by comparing content against a database of Internet addresses, and in some cases, a words and phrases list. A filtering program, depending on how its configured, can allow or prevent access, log activity, send warning messages or terminate the Internet connection. Client-side filters can also control the transmission and reception of certain words and phrases, including personal information. Some client-side filters provide activity logs that report sites visited, personal information sent and time spent online – for each member of a household – which can be useful for ensuring that rules are followed.

Many people think that if a filter is installed, it automatically blocks access to content. In many cases, parents choose other options that don't involve blocking at all. A good client-side filter carries out a parent's specific wishes and follows a child's online activities regardless of which ISP, search engine or other Internet program is used. Some client-side filters provide all of the features mentioned above, others offer more or provide less. While a client-side filter requires more involvement, it usually provides more flexibility than other filtering options.

Alternatively, server-side filters, which are offered through Internet Service Providers, control content before it reaches an individual computer, requiring little or no involvement from the parent or caregiver, which many parents prefer. Though less so than client-side filters, server-side filters do offer some measure of choice, particularly by age group and category of content, but because they are built to address the needs of a large group of users, they are unable to match a client-side filter's granular controls. Some parents and kids who access the Internet through a filtered ISP can't always access content they need, and are forced to either turn off the filter or choose another ISP that doesn't make the filtering decision for them. Kids can bypass server-based controls by getting their own ISP accounts or using other tactics that exploit security holes, but client-side filters can also be vulnerable.

It is important to note that one approach is not necessarily better than the other; each has its own strengths and limitations. Parents need to choose what is right for them. In some instances, consumers can benefit from using the solutions together, but it is important to know exactly what is gained or lost by combining the two.

Whichever option a parent chooses, the importance of parental or caregiver responsibility must not be underestimated. Using a filter doesn't mean that parents shouldn't continue parenting, it simply makes their lives a little easier and offers some peace-of-mind, by serving as an electronic extension of their own values system. It is crucial that parents ALWAYS pay attention to what their kids are doing online. They need to make sure that the filtering program is operational and hasn't been bypassed by their young "technical wizard." They also need to consider accessing a filter's logs and a browser's history file to see if their rules or instructions have been violated. By paying attention to their child's behavior and going online themselves to learn what their children are doing, parents and caregivers have the means to step in when necessary.

Client-side filters are often accused of failing to be 100% effective. Those of us, who have been in the industry for several years, understand that it is impossible to please 100% of the people 100% of the time. We do, however, listen closely to our supporters and our detractors so that we can adapt our technology to address their concerns. New tools are emerging that will allow the filtering programs to do a better job of keeping up with the massive growth of Internet content, however, it is impossible to capture every site that may be considered inappropriate for children. Innovation is a constant in the technology industry and filters continue to benefit greatly from constant feedback.

Client-side Filtering and the First Amendment

The notion that client-side filters are incapable of supporting the First Amendment is false. The filtering industry continues to be plagued with First Amendment controversy, because the products have been known to block access to unobjectionable and/or constitutionally protected content, depending on the way they are used. The vast majority of the filtering industry pays lip service to the First Amendment, but fails to provide tools that actually allow individuals and organizations to choose for themselves what content is suitable or not for their children.

Since offering the world's first Internet filter in 1995, Net Nanny has successfully navigated the turbulent waters associated with protecting children online and preserving one of our most cherished rights – the right to free speech. From the beginning, we recognized that while pornographic, violent and other objectionable material would continue to grow; it would never overshadow the overwhelming amount of positive material available to benefit children. Giving parents and caregivers the tools to steer their children toward the positive and away from the negative, without jeopardizing the rights of other Internet users, was never seen as impossible. We saw it as the “best of both worlds.”

Net Nanny subscribes to the belief that filtering products must not only protect children online, but also respect the First Amendment. Products like ours demonstrate that it is possible to achieve both of these goals by providing full access to, and control over, the database of Internet addresses and words and phrases. While some members of the filtering industry give users the ability to choose which categories of content to block, this should not be confused with full disclosure.

While it is necessary to build a database and keep it updated, consumers should have the ability to analyze each and every site in the database and allow or disallow access based on their own needs and value systems. Consumers should not be put in a box that forces them to adapt to someone else’s idea of what is best for their situation. It is not a corporation’s right to arbitrarily decide what is best for people who use filtering programs. We must give consumers the power to determine that for themselves. In a free society choice is key, unless perhaps the content is illegal, such as child pornography.

Some companies choose to view their databases as proprietary and therefore shield them from their customers. Their decision may be based on their business models, because many of them make money charging subscription fees for database updates, or other reasons that support their corporate philosophies. It remains clear that filtering solutions, which fail to provide full disclosure, will always be criticized - so much so that even solutions like Net Nanny, which DOES provide full disclosure, occasionally gets lumped with all of the rest. It just makes sense to give people complete control over a filter’s database. To do anything else simply detracts people from seeing the valid need for filters.

It is technically possible to filter sites according to a certain set of standards – they could be legal or they could be personal. The difficult proposition is reaching agreement about what constitutes obscenity and what constitutes content that is “harmful to minors.” The technology, itself, is capable of housing just about any sort of content that a person, group or law requires – the trick is properly identifying it.

Filtering criteria and ratings systems

Another important aspect to consider is the criteria used to build a filter’s database. What kind of agenda is a filtering company promoting? Who are the people making decisions about which content should be included? When dealing with child safety, we must know on what grounds an individual is considered an expert? No matter what their qualifications, people have agendas and have been known to break the law regardless of their profession or whether they have children. It is for these and many other reasons that consumers, who use filtering programs, must remain vigilant. People directly responsible for protecting children should always make the ultimate content decision.

Ratings systems are also problematic. These systems, which categorize and identify Web sites based on a common set of criteria, sound feasible in theory but are less so in the real world. They raise concerns similar to those associated with building databases. Who is making the rating decision and can this approach address the wide variety of needs and sensibilities that exist within the global Internet community? What are the criteria for rating sites? Do they take into account cultural, and societal norms? What is acceptable in this country is not necessarily going to be accepted in a more conservative or liberal culture. It remains to be seen whether ratings systems will catch on, but the filtering industry should continue to work closely with those who are developing a ratings model and incorporate accepted technical standards to increase consumer options.

Cooperation with Internet Industry

Constant technological changes can and do affect the performance of filters from one day to the next. It is our hope that companies who produce chat, instant messaging systems, search engines, browsers and other Internet technologies will step up their efforts to share important technical information with child safety software vendors. Just as the telecommunications industry depends on common standards and agreements to deliver superior voice and data services, the filtering industry needs cooperation and disclosure from a variety of Internet software vendors to continue to provide effective solutions. In an intensely competitive environment, cooperation often takes a back seat to proprietary goals. When it comes to protecting children online, the industry must make more of an effort to ensure technical compatibility. Communication *can* be enhanced without jeopardizing market advantage. We are encouraged that a few prominent industry leaders recently agreed to increase their cooperation, and we look forward to more companies doing the same.

How can the government help?

Many tools are available to help protect kids online, but most people aren't informed enough to know whether they need a filter or that filters are useful. Technology is often more daunting to parents than to kids. Before parents can even feel comfortable taking an active role in protecting their children online, they need to understand the problems associated with the Internet.

Firsthand experience has taught our company that education is key to protecting children online. It must focus not only on children, but on parents as well. Each month, we team up with law enforcement and other computer security specialists to teach a free eight-hour class called the "Internet and Your Child" to parents, teachers and law enforcement. These people are interested in Internet safety and practical tips for improving children's online experiences. Some of them have computer experience and understand the dangers associated with the Internet, but most do not. The curriculum covers a wide variety of Internet concerns and the major technical methods for managing Internet access. It maintains neutrality by providing objective information and encouraging attendees to make up their own mind about ways to control the Internet. One of the most significant resources we use is GetNetWise – an excellent online resource for information on tools, reporting trouble and accessing positive online content.

The classes have a secondary benefit in that they help to create a lasting community network of concerned people who come from different backgrounds. Through IYC's Web Community on MSN, attendees continue to benefit from additional knowledge sharing and camaraderie among IYC participants across the country. In every sense of the word, this is a grassroots public/private partnership that is supported by the goodwill of a handful of people and companies. While it is making a very positive impact, it needs additional resources to meet the overwhelming demand for Internet training.

The government should make it a priority to encourage the growth of educational programs such as IYC through endorsements and the creation of public-private funding partnerships. It should require that straightforward information on current and proposed laws be posted in a central location that is easily accessible, so people are up-to-date on the legal climate. It should also expand funding for law enforcement to ensure that it has the latest technology and training to fight crime. Over 90% of the police departments in the U.S. have 50 officers or less making it difficult for departments to expend the resources necessary to meet demand. Federal, state and local agencies need to be encouraged to find more efficient ways to work together, and with their counterparts overseas. It is crucial that they learn more successful ways to navigate jurisdictional lines that have been complicated by the Internet. And finally, the government should continue to promote user empowerment technologies that put control into the hands of individuals. They want and need protection that suits their own situation. Free enterprise ensures that these technologies are available and that they will continue to improve.

Summary

It is my hope that people involved in protecting children and the integrity of the Internet will seek to find a middle ground where both goals can be met through accurate product and issue analysis, sharing of constructive ideas and a willingness to look beyond individual agendas to achieve a workable solution. The alternative is more confusion for consumers and the danger that both child safety and our constitutional rights will fall through the cracks. Like most things, client-side filters are not perfect, but they will reach their potential if they are built with constructive input from people who care. Ideally, their potential will be reached when people understand that filtering tools should never replace parenting in the digital age, but rather assist it. With the proper combination of technology, education and policies, we will succeed in protecting children online and preserving the integrity and openness of the Internet.

Thank you.