Testimony of Kevin Blakeman

Chairman Telage, thank you and your fellow commissioners for offering me the opportunity to testify before you today.

My name is Kevin Blakeman. I am president of U.S. Operations for SurfControl, located in Scotts Valley, California. We have been at the forefront of the Internet content filtering and monitoring business from its earliest days, and with the acquisition of SurfWatch and CyberPatrol, we are in the unique position of servicing the home, education and business marketplaces.

But the World Wide Web is a much more challenging place today. The number of new web sites and pages that appear each day are far too many for anyone to keep up with.

Filtering at individual computers is certainly a technology that gets a great deal of attention, and it is one of the initial technologies we offered to our customers. Typical filtering is limited to sites on the World Wide Web; it can block certain specific sites or types of sites. But those are hardly the only places online where inappropriate material may lurk. Keeping children safe also means watching e-mail, file attachments, or downloaded material like video files or MP3 audio files.

More advanced filtering technology lets families block inappropriate material in all these guises, not just web sites. For example, parents concerned that their kids might be illegally downloading music from the Internet, such as MP3 files that are circulated without the consent of the copyright holder, can set advanced filtering software to watch for those file types. If the child using the family computer tries to download any file with an MP3 extension, the filter will block the attempt. If a child finds a legitimate MP3 file they'd like, they can get past the monitoring in a simple way: ask Mom or Dad for permission, returning power from the computer to the family.

Now, filtering alone might not be able to "see" everything coming into a computer. It is possible a file type or a web site that hasn't been put into the filtering list yet could get past. But by using another powerful technology, that of monitoring, schools, libraries and other places can add another layer of checks to see if inappropriate material is making its way onto the computer screens of children.

Monitoring technology works like this: the network manager or other person responsible for overseeing computer use installs "packet sniffer" technology at a point in the network where traffic flows from the connection to the Internet to individual computers. The packet sniffer technology looks at any TCP/IP traffic flowing past it – not just web pages, but file downloads via FTP and the like – and creates a picture of this traffic it can "see." It is possible to do this without interrupting traffic or disrupting the flow of data, things that would annoy users and perhaps cause system managers to turn the monitoring off.

A simple analogy is that of a traffic officer who stands by the side of the highway and observes the situation, recording it and reporting it when appropriate. If instead the officer stood in the middle of the highway, he would no doubt slow everything down.

When the monitoring software "looks" at the traffic information it has monitored, it can quickly place the sites visited, files downloaded and so forth into one of several categories that have been previously defined by the system manager. The monitoring software reports on everything from excessive Internet use to visits to sites, perhaps unblocked by filtering, that fall into inappropriate categories. This enables a system manager to quickly pinpoint possible improper Internet activity by a user – an active, human intervention that complements a rule-based, up-front filtering operation.

The combination of monitoring and filtering is already working in businesses to ensure that workers are using the Internet for business purposes, rather than personal uses. The same technology can be applied where children are the expected users of the Internet.

This system could be employed at a school, for example, where an acceptable use policy for the Internet has been adopted. Filtering can ensure that previously identified inappropriate sites, file types, e-mail attachments, video clips and the like are excluded from view at the school. And by examining the reports from the monitoring software, the responsible school official can see if other material, not already identified in the filtering list, has found its way into the school's computers in violation of the policy. It makes it fast and easy to take the action necessary to ensure the school's policy is followed.

Another technology that will become even more important in the future is the addition of artificial intelligence techniques to compliment and supplement monitoring and filtering.

Artificial intelligence makes it possible not only to categorize sites as potentially inappropriate much more quickly than the "spider-to-human" method, but also makes it possible to maintain filtering in useful ways including across the full services of an ISP or to create filtered search engines.

Any form of Internet filtering is dependent on the quality of the list it uses in the process, and the web is expanding at such a rate as to make the job very difficult. Today many filtering techniques rely on large-scale human interaction to properly characterize the thousands of new sites that appear on the Internet daily. Most of the time, a "spider" or "crawler" program is used to prowl the Internet looking for new sites, and passing their identities onto humans to categorize. It is a very time-consuming process.

Artificial intelligence can act as an intermediary in the process, by taking the data produced by the spider program and analyzing it, properly categorizing it. Human eyes can then take the last step, verifying that the artificial intelligence program has done the job properly.

This technology greatly decreases the amount of time needed to update the lists upon which filtering systems are based. For ISPs, the technology means that once it has

implemented filtering, it can enhance the list it uses automatically. ISPs will be able to offer customers, with a reasonable degree of assurance, several levels of protection from inappropriate sites. Users need not buy, install, and continuously upgrade the technology themselves.

Artificial intelligence can also be built into the ISP's software installed at the homes of its customers, enabling families to build a bigger database of sites to be filtered than the standard coming from the ISP. This is a step beyond the "customizable list," where the consumer adds specific sites to a list addendum: the AI engine, based on parameters specified by the user, builds the custom list for the family. And the technology is equally adept at creating a "white list" as it is a "black list:" families could easily create a limited set of sites that parents feel fully comfortable allowing their kids to use.

In fact, artificial intelligence technology can enable ISPs to offer families a variety of filtering options for each logon – in other words, for each member of the family. Mom can use her secret password to tell the ISP – not the home PC – how to construct a filtering database for Bobby. Mother and son can use the same computer and same ISP, yet have starkly different filtering lists. Plus, having the list kept and updated at the ISP makes it far more difficult for Bobby to hack around the home PC looking for a way to skirt the filtering system.

Today, artificial intelligence is constrained by the speed of the available hardware. But in time, it will be possible to use this technology – whether at the ISP level or individual user level – to create "real-time" filtering, where even if a site is not on any list, it can be evaluated, categorized, and blocked if necessary – and without performance penalties to the user.

Over time, advanced filtering, monitoring technology and the use of artificial intelligence by ISPs and individuals will make the job of keeping children and inappropriate content far easier, and far more comprehensive.

Thank you for your attention.