Statement of Timothy W. Cranton
Associate General Counsel, Worldwide Internet Safety Programs
Microsoft Corporation

Before the United States
Commission on Security and Cooperation in Europe

"Combating Sexual Exploitation of Children:
Strengthening International Law Enforcement Cooperation"

June 17, 2008

Chairman Hastings, Co-Chairman Cardin, and honorable Members of the Commission, my name is Tim Cranton, and I am Associate General Counsel of Worldwide Internet Safety Programs at Microsoft. Thank you for the opportunity to appear before you today to discuss strengthening law enforcement cooperation to more effectively combat the sexual exploitation of children. The Internet has brought us tremendous advances, which have promoted community and cultural interaction, created new economic opportunities, and fostered individual autonomy and freedom around the world. But the Internet also has created new avenues for criminals, which has exacerbated the problem of child exploitation and other crimes.

The Internet facilitates online child exploitation in a number of ways. The Internet gives criminals preying on children a new, anonymous route to identify, groom and lure children to exploit. For those who create, view and distribute images of the sexual exploitation of children, it provides a global marketplace and community that makes it easy and cheap to distribute, share, and find all types of child pornography and abuse images. At the same time, the Internet also makes tracking these forms of child exploitation harder for law enforcement. Criminals can use new and sophisticated technical tools to avoid detection. And because the Internet spans national boundaries, a child predator's activities can easily occur in several countries simultaneously, outside the jurisdiction of any one law enforcement agency.

This global aspect of online child exploitation necessitates the conversation we are having here today. Global problems require global solutions, which means that different nations and the public and private sectors must work together to combat child exploitation. This cooperation demands robust information sharing about child predators and child exploitation investigations, between different law enforcement agencies and between the private sector and those agencies. Sharing this information is critical both so that agencies can cooperate on individual investigations which span national boundaries, and so that they can find the links between seemingly unconnected cases around the world. The private sector — especially the technology sector — is well equipped to work with government to facilitate that cooperation.

Microsoft is deeply and broadly engaged in efforts to address child exploitation and other Internet threats through our global Internet safety programs. These programs follow a five-part strategy that includes:

1. developing technology solutions;
2. advocating legislative and policy reform;
3. supporting broad education and awareness programs;
4. forging strong cross-industry and public-private partnerships; and
5. facilitating strong civil and criminal enforcement.

To advance these priorities, we have established an Internet Safety Enforcement Team within Microsoft's Legal and Corporate Affairs division. We are dedicated to developing and implementing innovative programs to combat online child exploitation, as well as other Internet threats.

Today, I will focus on how private industry can help the public sector combat child exploitation online. These efforts fall into three general categories:

- **Tools:** Developing technology tools to help law enforcement share information and collaborate more effectively, like the Child Exploitation Tracking System;
- **Training:** Providing education and training for law enforcement throughout the world on computer-facilitated crimes against children; and
- **Partnerships:** Forming cross-industry and public-private partnerships that focus on collaboration and building resources that enable such collaboration.

At Microsoft, we see private-sector efforts as complementing the work of the public sector. We each have our own strengths we can contribute to the fight against child exploitation online, and we will have the greatest success if we can work together to maximize each of our respective resources. In that vein, I will close my testimony today by highlighting some of the ways in which we believe the members of this Commission can help foster increased cooperation and information sharing between the public and private sectors.

The Private Sector's Role In Developing Technology Tools

As a technology company, Microsoft is in a unique position to provide the technical know-how to address child exploitation and pornography. Our technology efforts include developing technology that identifies, removes, and refers illegal content; clearinghouse technology that helps analyze, process, and compare information about online child exploitation; and investigative technology that facilitates law enforcement investigations, prosecutions and convictions. I will address each of these efforts in turn.

Identifying, Removing and Referring Illegal Content

First, we have designed and implemented tools within our online services that identify possible child pornography and other illegal content. We then report instances to the National Center for Missing & Exploited Children ("NCMEC") for investigation, pursuant to the Victims of Child Abuse Act. Microsoft also follows the guidelines of the United States Internet Service Provider Association in reporting the facts or circumstances of apparent child pornography to NCMEC, including providing samples of the images uploaded. We also maintain a customer complaint capability to review reports of child pornography or exploitation, and similarly remove offending sites and report them to NCMEC and other appropriate authorities.

Clearinghouse Technologies

Second, we are working with our industry partners to develop technology to assist NCMEC with handling the information it receives from Microsoft and other service providers pursuant to these processes. Specifically, Microsoft joined with NCMEC, AOL, EarthLink, Google, United Online, and Yahoo! in 2006 to establish the Technology Coalition to Fight Child Exploitation, which is working to establish a clearinghouse at NCMEC that will serve as a secure, third-party repository for known illegal images of child exploitation. Secure repositories are essential because they allow service providers to compare electronic signatures of suspect images to those in the repository, facilitating automated filtering for child pornography. They also help prosecutors prove cases in court by providing evidence to rebut a defendant's claim that an image was computer-generated, or that the person shown was not a child.

Tools to facilitate law enforcement investigations

Third, we use our technical expertise to create technological platforms that facilitate investigations by helping law enforcement to organize, share, search, and store data, and by making investigations easier and more efficient. These efforts and tools are especially important because they target the Internet's international and interjurisdictional nature — perhaps cybercriminals' biggest advantage on the Internet. I would like to spend a few minutes highlighting three of the tools we have developed that help law enforcement fight child exploitation online: (1) the Child Exploitation Tracking System, (2) Microsoft Office Groove, and (3) the Computer Online Forensic Evidence Extractor.

(1) The Child Exploitation Tracking System ("CETS")

CETS was developed in response to a plea from Paul Gillespie, a police officer overseeing the Toronto Police's child exploitation unit. Mr. Gillespie noticed that the Internet was giving sex offenders greater access to potential victims. He sent Bill Gates an email back in 2003, describing the problem and asking for our help combating it. His email struck a chord, and Microsoft Canada sent a software engineer named John Hancock to meet with Gillespie's investigators and see how we could help. Mr. Hancock noticed that although the investigators were using the Internet in incredibly sophisticated ways, they did not have specialized tools to help them connect and track data from different investigations and jurisdictions. Microsoft Canada set out, with the Royal Canadian Mounted Police and the Toronto Police, to create such a system, and the result was CETS.

CETS was launched in 2005 in Canada. It allows different law enforcement agencies from around the world to access and collaborate on child exploitation cases in a secure manner, and it lets them tailor their information sharing to the limits of the local laws and clearly defined sharing agreements in place. It also enables agencies to upload information they obtain in investigations and automatically compare it to information from other investigations to find connections. Investigators can capture, share, and search information at all stages of an investigation, and as the CETS database grows, it becomes increasingly valuable. It also includes built-in integration with Microsoft Virtual Earth, so that law enforcement can locate sites of interest on a map and find other records and points of interest, such as schools or community centers, nearby.

CETS proved its significance even before it was officially launched: while it was being tested in 2004, it uncovered a link between seemingly unrelated child pornography cases on different continents, ultimately resulting in the rescue of a four-year-old child in Toronto. CETS has not let up since then: Mike Manning of the UK's Child Exploitation and Online Protection (CEOP) Centre says that "given the fact that online investigations are not restricted by geographical borders, the capacity of CETS to store, retrieve, and cross-reference this information is invaluable." In the UK alone, relying on CETS's multi-agency, technically sophisticated approach, the CEOP Centre has made 240 arrests, dismantled three international pedophile rings, and rescued 138 children who were victims of child predators — all since April 2006. Other countries have seen similar successes. Law enforcement have quickly embraced CETS; since its launch in 2005, it has been deployed in eight countries — Canada, Indonesia, Brazil, Italy, the United Kingdom, Chile, Romania and Spain. A total of 1,236 law enforcement officers have been trained on CETS to date. And Microsoft is working with seven other countries to support further expansion of CETS.

(2) Microsoft Office Groove

CETS helps police find connections between seemingly unrelated investigations, but information sharing is also critical within individual investigations. In the Internet age, a single investigation can frequently span multiple countries and continents, and as child pornography increasingly becomes a business, this problem will only increase. Microsoft Office Groove addresses this difficulty by allowing widely dispersed teams to work together dynamically, effectively, and quickly, even when team members work for different organizations that use different computer networks with incompatible security systems. Members can work remotely or even offline and still have access to common data and software.   Groove is a commercial product that is used by teams of all kinds, but it is well suited to aiding widely distributed law enforcement investigations, and we include it with the CETS software and have worked to integrate the two.

Microsoft has also contributed Groove software and licenses to Interpol, which uses the software to link together agencies working on international child exploitation investigations. One officer described Groove as "the number one software for … investigating crimes against children." He credits Groove for allowing international teams to identify and rescue at least 20 abuse victims much more quickly than without the software. One example of that occurred when a child predator turned up unexpectedly in Asia. Groove enabled the local police to obtain access in less than an hour to hundreds of megabytes of data and numerous tools, which allowed them to collaborate quickly with investigators in Europe.

(3) The Computer Online Forensic Evidence Extractor ("COFEE")

These tools help law enforcement share data they have uncovered in investigations, but law enforcement also need help in obtaining that data in the first place. We developed COFEE to address this need. Preserving information can present difficulties for law enforcement, since forensic analysis on computers usually must be performed in a lab. This requires police to shut down power to the machine, possibly losing valuable information. COFEE is a software package which fits on a USB drive and allows law enforcement to automate more than 150 forensic commands on a live computer system and save the results for later analysis. In a pilot program, Microsoft has provided COFEE for free to over 2,000 select law enforcement officials worldwide. The response has been highly enthusiastic, and we have now closed the pilot program and are working on plans to roll COFEE out to law enforcement users more widely.

***

Filtering and identification technology, robust clearinghouses, and with tools and systems designed to facilitate law enforcement investigations represent examples of industry bringing our technical expertise to bear in the global fight against cybercrime. We have had significant success in the technological realm thus far, and we will continue to devote our efforts in this area.

The Private Sector's Role in Offering Training and Support

In addition to offering technology tools, we can contribute to the fight against child exploitation online by educating and training law enforcement officers throughout the world about the technical aspects of Internet crimes and investigations. To this end, Microsoft has partnered with the International Centre for Missing & Exploited Children ("ICMEC") and with Interpol to sponsor law enforcement training sessions on computer-facilitated crimes against children. In these sessions, officers learn about investigating online crimes against children, identifying suspects, dealing with victims, managing complex international investigations, and preventing further abuses.

In conjunction with many of these training sessions, we have coordinated public roundtable discussions with regional and local officials to raise awareness of child protection issues in the online environment. These discussions typically involve featured speakers and question-and-answer sessions regarding computer security and Internet-related crime in the host country or region. Since our law enforcement training initiative was launched in December 2003, over 30 regional sessions have been held, teaching nearly 3,000 law enforcement officers from 111 countries.

These trainings have contributed to developing the expertise and facility of law enforcement in numerous successes around the world. For example, in a worldwide investigation code named "Operation Achilles," police rescued 20 children and raided and arrested more than 20 pedophiles across six countries. The operation, which was carried out by the Australian Queensland Police, involved numerous countries that have sent participants or presenters to the training. Similarly, the week following a training session and high-profile roundtable discussion held in Buenos Aires, Argentina, over 200 federal police officers conducted more than 20 raids in Buenos Aires. These raids led to the discovery of a large child pornography band originating in Norway, which has since been dismantled. And since the April 2005 training in Madrid, Spain, several large child pornography investigations have resulted in numerous arrests, many the result of a coordinated investigation known as Operation Xuxa. In the first half of 2007 alone, Spanish law enforcement investigated 70 individuals suspected of sharing and posting images or videos of children as young as nine years old.

The Private Sector's Role in Forging Partnerships to Facilitate Information Sharing

Along with creating technology tools and providing training and support that help law enforcement combat child exploitation, we believe industry can assist the public sector by building resources and forming partnerships that focus on collaborating to fight child exploitation online. We have worked extensively with NCMEC and ICMEC, for instance, and we support and commend their important work.

One example of a powerful collaboration resource is the Law Enforcement Portal, which Microsoft launched in 2006 to provide law enforcement with online access to information and forensic support. The Portal provides field officers with real-time technical support and training, allowing law enforcement officials to securely leverage

Microsoft resources from any location at any time of day. It also contains useful reference materials for law enforcement performing cyber-investigations.

Global hotlines are another important information-sharing resource. Hotlines serve a number of important functions in the battle against online child predators. They provide Internet users with an accessible mechanism to report suspicious activity on the Internet. They allow the private sector to use our expertise and resources to investigate and confirm reports of illegal content. And they let investigators trace the origins of illegal content, refer the matter to law enforcement agencies in applicable countries, and, when appropriate, issue a takedown notice to the Internet service provider.

Of course, national hotlines operating in isolation would be insufficient to combat the international problem of online child exploitation. Accordingly, Microsoft has partnered with the International Association of Internet Hotlines ("INHOPE") since its formation. To date, INHOPE consists of 33 member hotlines in 29 countries — including NCMEC's CyberTipline in the United States — that respond to reports of illegal content in order to make the Internet safer. Through a Memorandum of Understanding signed in April 2006, Microsoft has committed to provide financial backing, technical training, and software licenses to INHOPE.

Microsoft also is a founding member of various partnerships which aim to fight child exploitation by bringing companies together to combine resources and expertise. One example is the Technology Coalition, which I described earlier. Another is the Financial Coalition Against Child Pornography, which was launched in March 2006 thanks to the leadership of NCMEC and Senator Richard Shelby (R-AL). Comprised of leaders in the banking and payments industries, as well as Internet services companies, it is a collaborative effort aimed at cutting off child pornographers from sources of income for their trade, increasing private sector information sharing, and, ultimately, eradicating commercial child pornography. The Financial Coalition has enjoyed significant successes in disrupting the payment stream to commercial child pornographers.

The Virtual Global Taskforce ("VGT") is another successful partnership, bringing together law enforcement officials in the United States, UK, Australia, Italy, and Canada, as well as Interpol, to pursue efforts to make the Internet safer for children. Through VGT, Microsoft has worked with law enforcement officials to develop training programs. Additionally, Microsoft has worked with VGT and ChildNet International to develop an educational program on online safety for children, teachers, and parents entitled "Getting to Know IT All," which was the first campaign of its kind in the UK, and will soon be expanding to Australia.

By drawing on our collective knowledge and ideas, these resources can be a powerful weapon against those cybercriminals who seek to exploit children online.

How The Commission Can Help Facilitate Public-Private Partnerships

Microsoft is committed to working with the public sector, in all the ways I have described, to protect children from online predators. But we know we can do more together on a global level to prevent child exploitation online. We believe the members of this Commission are in a good position to foster increased cooperation between the public and private sectors. I would like to highlight three things you can do to help.

First, we need to strengthen laws that encourage information sharing between the private and public sectors. There are several facets to this information sharing. As an initial step, countries should pass laws that provide minimum baselines for what is illegal, so that law enforcement can be certain that content is illegal before launching international investigations. The Council of Europe Convention on Cybercrime provides an excellent foundation for this and should be ratified around the world. In April 2006, Microsoft joined ICMEC in announcing support for model legislation against child pornography, which proposes, among other things, to incorporate specific child pornography-related offenses into nations' penal laws and institute appropriate criminal sanctions for child pornography.

We also need laws that require private companies to report instances of child exploitation they discover. ISPs already face that obligation in the United States, but non-ISP companies in the US that run across evidence of child exploitation are not required to report it. Similarly, many other countries have not implemented this solution. Without a reporting obligation, child predators will discover and use services offered by companies that do not report. Requiring reporting will mobilize additional companies and resources to the fight against online crimes.

We also need better mechanisms for private companies to report suspected child pornography to foreign government authorities or Interpol. Currently, a company that comes across evidence of child exploitation can report that evidence to the US government, but foreign reporting is hampered by the lack of clear legitimate reporting mechanisms. Such mechanisms would require the involvement of both the United States and the recipient country. Countries should work to establish laws and treaties that provide for such referrals.

Finally, we also need laws that allow law enforcement to share investigation details with groups like the Financial Coalition and Virtual Global Taskforce, while still protecting the privacy of investigations. Such laws would help us help law enforcement by enhancing these coalitions' ability to shut off payment streams and build improved blocking tools, for example. The members of this Commission are in a perfect position to encourage and lobby other countries to enact these types of legislation.

The second thing that would help is legislation that ensures that industry has the ability and the incentives to help law enforcement without being penalized for that assistance. Companies should not face potential legal liability for reporting possible child exploitation cases to the government. United States law currently provides immunity to Internet service providers that report child pornography to authorities, but similar laws are needed for other types of companies that may come across child pornography, and for companies in other countries. No businessperson should have to hesitate in reporting crimes against children for fear of civil liability. Carefully tailored laws limiting liability for actions taken in the fight against child exploitation should be enacted around the world.

Third, greater resources are needed for law enforcement to enable them to take advantage of industry efforts. Microsoft has invested more than $10 million in CETS and contributed over $2 million to training law enforcement on how to investigate computer-facilitated crimes against children. Of course, we are eager to do our part to fight child exploitation, and we make our training sessions and tools like CETS and COFEE available to law enforcement agencies free of charge. But law enforcement needs more resources, including more trained investigators, to take full advantage of these systems.

Likewise, resources are needed to fund the development of new tools and for education about the threats posed by child predators on the Internet. Child pornography has become a big business on the Internet, with worldwide revenues estimated at $20 billion; significant money is needed to take on a problem of such a large size and scope. One proposal would allocate more than $100 million a year toward fighting online child exploitation. This is a fight that requires substantial resources, and we urge Congress to provide this level of funding. Other countries similarly need to come forward to support cooperative efforts and fight child exploitation.

Conclusion

Over the last decade, child pornography and child exploitation have become big business, and our approach must adapt to that reality. The Internet makes it easy to transfer information instantaneously and anonymously, and child predators take advantage, using sophisticated technology to evade detection and profit from their crimes. Neither government nor industry has the ability to defeat them alone, so we must work together.

Our collaborative efforts have made good progress so far, but more can be done. We must recommit ourselves to strengthening the public-private partnerships that can help us find connections between seemingly unconnected data and make such a difference, and to devoting the resources needed to taking on the fight. We at Microsoft are ready for this challenge. We look forward to continuing our work with others in industry, law enforcement, and the international community to limit child exploitation on the Internet to the greatest extent possible.