

BEFORE
THE COMMITTEE ON COMMERCE AND ENERGY
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
UNITED STATES HOUSE OF REPRESENTATIVES

“MAKING THE INTERNET SAFE FOR KIDS: THE ROLE OF ISPS AND SOCIAL
NETWORKING SITES”

WRITTEN TESTIMONY OF
JOHN D. RYAN
CHIEF COUNSEL
COMPLIANCE AND INVESTIGATIONS
AOL, LLC.
DULLES, VIRGINIA

June 27, 2006

Mr. Chairman and members of the Committee, my name is John D. Ryan, Chief Counsel at AOL, where I oversee our efforts to assist law enforcement and keep criminal activity off our networks. Prior to joining AOL, I was a prosecutor in New York where I investigated and prosecuted numerous high tech crimes, including crimes against children. I am a founding member of the Electronic Crimes Task Force in New York, which has been used as the model for the cooperation between law enforcement and industry in the prosecution of electronic crimes.

AOL applauds the efforts of this Committee in addressing the twin scourges of child pornography and child predation on the Internet. AOL has been fighting the spread of these plagues both on our network and on the Internet for over a decade. The single guiding principal for AOL has been and continues to be the protection of children online. AOL has pioneered the use of innovative technologies to protect children online. It has implemented industry leading practices and policies that have been both adopted by others in the industry and included into state and federal legislation. AOL has staked its brand and reputation on providing a safe haven for children online. For AOL, these efforts make good business sense, but more important, are the right thing to do.

As this committee is well aware, these crimes represent a particular challenge because they are facilitated by computers and the Internet. The challenges created by technology should be addressed by technology as well. Three years ago, AOL implemented extremely effective technologies to identify and remove abhorrent images of child pornography and to eliminate their transmission on its networks. AOL developed a process that creates unique digital signatures from apparent pornographic images of children and uses those signatures to eliminate further dissemination of those images. AOL has assembled a library of those image signatures and, if AOL discovers that someone is trying to send a file over our network with a signature from that library,

AOL prohibits the transmission of that file and refers that image to the National Center for Missing and Exploited Children (NCMEC) to be investigated and prosecuted. Once the signature of the image is identified and referred to NCMEC, AOL deletes all record of the image and only retains the signature for future identification of bad images.

At AOL we believe that proven technologies such as these make it harder for criminals to use the Internet to commit these crimes against children. AOL is committed to developing and deploying more promising technologies to take back the Internet from those who would exploit or harm our children. AOL is also committed to working with industry develop and implement these technologies widely. As I will discuss in more detail later, AOL has assembled a coalition to focus on these efforts.

The primary objective at AOL is to ensure that children never become victims of online predators or become exposed to inappropriate content. Over the past decade, AOL has developed state-of-the-art parental controls that give parents the ability to block their children from receiving harmful content. AOL Parental Controls are broken down into three age categories: Kids Only for ages 12 and under; Young Teen (13 – 15); and Mature Teen (16 and 17). The controls provided include the ability to block email, instant messages, or chat with unknown persons or specific individuals. Parental Controls also provide chat rooms, if parents enable such access, that are fully monitored by internal AOL enforcement teams.

AOL Parental Controls also have practical features to empower parents to manage their child's use of the service. There is a simple online timer to limit the amount of time a child stays on AOL. For AOL broadband users, AOL also provides Internet access controls for the PC, which will prevent a child from bypassing Parental Controls.

AOL Parental Controls do not merely restrict a child's access to potentially harmful encounters on the Internet, they provide positive alternatives with a complete range of age appropriate programming for parentally controlled accounts. For Mature Teens, AOL has state-of-the-art web filters that allow older teens to access a much broader range of content while still blocking offensive content. AOL filters are able to rate the content of pages in real time and only deliver those pages that are appropriate, while blocking offensive sites. This gives teens the flexibility to use the web while providing the maximum protection

AOL also has a feature called Web Guardian that allows parents to keep track of where their children visit and their activities online. Parents who subscribe to the service receive a list for every session on AOL detailing every website their children visit, which sites they tried to visit but were blocked from accessing, and how many emails and IMs they sent. AOL provides over 1 million AOL Guardian reports to parents every week.

AOL knows that there are individuals who send inappropriate content over our network or attempt to use AOL to lure children. From the beginning, AOL has included a visible and convenient "Notify AOL" button for members to report unacceptable behavior they encounter on our network to teams of trained professionals in the AOL

Members Services department. Among the items reported are images of child pornography. Since child pornography is contraband and illegal to possess or distribute, AOL realized over a decade ago that this material belonged in the hands of law enforcement so that it could be prosecuted. Beginning in the mid 1990's, AOL established contacts with state and federal law enforcement agencies throughout the United States to whom AOL could refer the child pornography images and other identifying information for follow up investigations and prosecutions. In 1999, this practice was codified into Federal law in 42 USC § 13032, which was subsequently amended to designate the NCMEC as the sole recipient for referrals of child pornography.

Congress, through 42 USC § 13032, directed ISPs to refer the facts and circumstances concerning all images of apparent child pornography of which they became aware to NCMEC. AOL consulted with NCMEC to determine what information was needed and what format would best facilitate the transmission of the information. As a result of that partnership, AOL became the first ISP to electronically transmit the referrals of child pornography. AOL went well beyond the strict mandates of the law and provided the offending image, the screen name associated with the image, and the zip code on the account. Through this process AOL ensured that law enforcement would have the offending image and all of the information necessary to send the case to the appropriate law enforcement agency for follow-up. The simple act of including a zip code eliminated days and weeks of lost time spent identifying and forwarding the report to the right agency for investigation.

The reports that AOL received from its members and the information observed in monitored chat rooms also uncovered attempts by pedophiles to solicit children. Rather than ignore this troubling information, AOL once again partnered with NCMEC to establish a child solicitation referral process, similar to the referral of child pornography. NCMEC shared its expertise in identifying predatory behaviors and trained AOL personnel to spot this behavior in communications they review. If a communication that is reported or observed in monitored chat rooms indicates the real possibility a child is being targeted online, AOL sends a report of the communication to NCMEC. In circumstances where the threat indicates the possibility that a meeting could take place within 72 hours, AOL sends the report directly to law enforcement in the location where the child resides. This approach is not mandated by any statute, but it is the right thing to do. AOL has been informed that in the 2 ½ years of its existence, this program has led to 153 arrests. That is 153 or more children who were protected from abuse at the hands of a predator.

AOL's early experience showed that pedophiles do not take nights, weekends, or holidays off. As a result, in 1996, AOL initiated a 24/7 law enforcement hotline. However, there was no law providing ISPs immunity for giving information to law enforcement without process in the event of life threatening injury. AOL instituted a policy by which law enforcement officers could obtain the information if they identified the information as necessary due to a life threatening situation. In the years that followed, AOL provided law enforcement with information to help hundreds of real and

potential victims of violence, including children. In 2001, the policies of AOL were reflected in Federal law in 18 USC § 2702, which allows ISPs to provide transactional information and content to law enforcement on a showing of risk of death or serious bodily injury to a victim.

When Congress passed the Nationwide AMBER Alert law, AOL reached out to NCMEC and became the first ISP to initiate an Amber Alert program by which AOL members can receive email alerts targeted to their area. To date, over 365,000 AOL members have signed up to receive Amber Alerts. This program is unique and innovative and again demonstrates AOL's unflagging commitment to use the power of its network to provide protection to its users and others.

AOL knows only too well that crimes on the Internet pose particular challenges for law enforcement. Police and prosecutors frequently need special assistance in dealing with the unique challenges presented by investigating computer and Internet crimes. AOL has a team of highly trained and dedicated professionals, including former prosecutors, to assist law enforcement on tens of thousands of cases per year. They provide information in response to law enforcement requests, answers officers' questions on what types of information would help their cases, and provide guidance on obtaining the right information.

AOL has demonstrated an ongoing commitment to deliver cybercrime, digital evidence, and computer forensic science education to police and prosecutors through out the United States. AOL personnel teach at the FBI Academy in Quantico, Virginia, in the FBI Cyber Investigations Techniques & Resources programs. AOL personnel also teach Immigration and Customs Enforcement (ICE), IRS, ATF, and US Secret Service agents at a similar law enforcement education course at the Federal Law Enforcement Training Center in Glynco, Georgia. Since 1999, AOL instructors have taught law enforcement education courses to the nation's criminal prosecutors at the US Department of Justice's National Advocacy Center (NAC) in Columbia, South Carolina eight to ten times per year. AOL has participated in the NAC's Justice Television Network (JTN), which has produced eight separate episodes dealing directly with AOL-related investigations within their "E-Vestigations" series.

AOL sits on faculties, panels, technical and scientific working groups, and committees within the National White Collar Crime Center, the National Center for Missing and Exploited Children (NCMEC), the National Center for the Prosecution of Child Abuse, the National Center for Forensic Science, the American Prosecutor Research Institute and the National Association of Attorneys General. Each of these organizations conducts law enforcement training in which AOL provides technologists and resources throughout the year. Starting in 2000, AOL committed to provide technologists to NCMEC's law enforcement training programs for investigators and prosecutors. Since then, thousands of agents, investigators, and prosecutors have heard the AOL law enforcement educational sections within the programs "Protecting Children Online for Investigators" (PCO) and "Protecting Children Online for Prosecutors" (PRO).

Given the global impact of the Internet, AOL has also trained international law enforcement officials at Interpol in Lyon, France.

Since 1995, AOL has offered to the government, at no charge, litigation support, as well as fact and expert witness testimony on criminal cases involving records obtained from AOL. Each day, AOL receives dozens of inquiries and requests from law enforcement officials who ask for assistance with the many aspects of computer/Internet related criminal cases. Each request for litigation support or testimony from a prosecutor requires hours of research, meetings, conference calls, and dialog with the investigators and prosecutors. AOL personnel perform pre-trial litigation support, custodian of records, nexus, as well as fact and expert witness testimony to assist the government. Frequently, two or more AOL employees are usually out of the office offering testimony in jurisdictions all over the United States. Many prosecutors have reported that their success at convicting computer/Internet related criminals would not have been possible without the assistance and testimony from AOL records, fact, and/or expert witnesses.

AOL devotes considerable resources to these efforts. While AOL does not provide its assistance for recognition, it has received numerous awards, commendations, and citations from the US government. Those include: the United States Department of Justice Commendation Award - October 1997; High Technology Crime Investigation Association Award - March 1999; Federal Bureau of Investigation - Exceptional Service in the Public Interest Award - March 2000; Federal Bureau of Investigations White Collar Crime Program Award and Special Recognition for Outstanding Support - April 2001; National Missing and Exploited Children's Award - May 2001, May 2002 and May 2003; Computer Crime and Forensics Symposia Excellence Award - August 2001; United States Department of Justice/National Missing and Exploited Children's Individual Corporate Award, 2004. United States Secret Service Award for Outstanding Service in the Public Interest, 2004; FBI and United States Department of Justice Award for its role in the International Online Child Sexual Victimization Symposium, 2004.

Although AOL has taken a leadership role in the development of best practices and solutions, we recognize that as technology evolves and criminals become more sophisticated, much more needs to be done. It is also clear that many members of this Committee are very concerned about protecting children and want more to be done. As it has in the past, AOL aims to rise to these new challenges and has developed a proposal to address these concerns in the most effective manner.

Specifically, AOL commits to: (1) voluntarily preserve all relevant records relating to a report by an ISP to NCMEC; (2) support a legislative grant of authority to NCMEC to send preservation letters to ISPs upon review and determination that the referred images are child pornography; (3) build and expand upon AOL's digital signature technologies and to share it with other industry colleagues to expand its reach; (4) investigate new and innovative technologies to make the Internet a dangerous place for predators but not legitimate users; and (5) most important, work with law enforcement to identify tools that will assist them in their critical work.

As a demonstration of our commitment, AOL has organized and joined with a team of companies, including Earthlink, Microsoft and Yahoo!, which are here today, to develop effective technologies to investigate and prevent child pornography online and also to provide financial and personnel resources to NCMEC to further these efforts. These measures will ensure that law enforcement has all of the necessary data resources and tools so that they can pursue a successful investigation.

I am aware of the ongoing discussions between the Department of Justice and industry concerning the merits of a statutory mandate requiring that ISPs retain large amounts of data about the user's activity online for up to 2 years. I believe that a careful assessment of these proposals will show that they are in fact counterproductive and the efforts to create this massive and costly database will fall far short of its intended goal. Warehousing of data requires the allocation of enormous resources to maintain and secure that data. Those resources would be better focused on supporting law enforcement in the investigation of real-time active cases. Additionally, creating such a voluminous database will actually frustrate law enforcement's goal of locating and identifying the suspects they are pursuing. As databases grow in size and complexity the risk of data corruption increases as well. As a result, the possibility of not finding the requested information increases as does the potential for a false match.

Finally, even the best efforts at creating these massive databases are destined to fall short of their desired goal because they are easily circumvented. There are thousands of Internet access points that would not be covered by this data retention net, including Universities and other academic institutions, libraries, governments, the military, employers, and tens of thousands of wireless hotspots. A determined predator need only utilize one of these services to avoid the net.

AOL has long partnered with law enforcement in combating online offenses against minors and we recognize that law enforcement has a critical role to play in dealing with the use of the Internet to victimize children. However, AOL believes that the best strategies and solutions for solving the crises of child pornography and child predation lie with technology companies such as those testifying before you today.

In closing, we are committed at AOL to dedicate whatever resources are necessary to create a safe and secure medium for our most vulnerable users: children. We look forward to working with the Committee, the Department of Justice, and other stakeholders to ensure that no child is victimized by the abuse of our medium.

#