WRITTEN STATEMENT OF HEMANSHU NIGAM

CO-CHAIR, ONLINE SAFETY TECHNOLOGY WORKING GROUP

Before the

CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE SUBCOMMITTEE

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

THURSDAY, JULY 15, 2010

PREPARED STATEMENT OF HEMANSHU NIGAM

CO-CHAIR, ONLINE SAFETY TECHNOLOGY WORKING GROUP
SAFETY ADVISOR, NEWS CORPORATION
FOUNDER, SSP BLUE

"PROTECTING YOUTHS IN AN ONLINE WORLD"

CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE SUBCOMMITTEE OF THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.
July 15, 2010

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, thank you for giving me the opportunity to address you today on the best ways that we can collectively protect youth online. I bring with me over 20 years of experience in safety in the online and offline worlds. I am the founder of SSP Blue, a safety, security, and privacy strategic consulting firm for online businesses. I am also News Corporation's Safety Advisor, having previously served as News Corporation and MySpace's Chief Security Officer from the birth of social media. Before coming to News Corporation, I set in motion a cross-company strategy for child safe computing and led a cyber enforcement team at Microsoft Corporation. And prior to that, I was Vice President of Worldwide Internet Enforcement against digital movie piracy at the Motion Picture Association of America. I have also served as a federal prosecutor against Internet child exploitation and computer crimes at the U.S. Department of Justice, an advisor to the COPA Commission, and an advisor to the White House's Committee on Cyberstalking. Finally, I began my career as a prosecutor in the LA County District Attorney's office, specializing in child molestation and sex crimes cases. And so, I speak to you from various perspectives in private industry, government, and law enforcement.

As co-chair of the Online Safety Technology Working Group, I had the honor of leading the mandate to review and evaluate:

1. The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children;

2. The status of industry efforts to promote online safety among providers of electronic communications services and remote computing services by reporting apparent child pornography, including any obstacles to such reporting;

3. The practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children; and

4. The development of technologies to help parents shield their children from inappropriate material on the Internet.

The OSTWG had representatives from nearly every facet of the child online safety ecosystem totaling more than 250 years of experience in online safety. Members were appointed from the Internet industry, child safety advocacy organizations, educational and civil liberties communities, the government, and law enforcement communities.

In order to best identify the best solutions for protecting youth online, the OSTWG quickly created four subcommittees to focus on each area we were asked to evaluate. These subcommittees were chaired as follows: Lawrence J. Magid of Connect Safely led the Education subcommittee, Michael W. McKeehan of Verizon led the Data Retention subcommittee, Christopher G. Bubb of AOL led the Child Pornography Reporting subcommittee, and Adam Thierer of the Progress and Freedom Foundation led the Technology subcommittee. Given the deadline of providing a report to Congress within one year of the first meeting, we set and followed a very strict timeline that began with an introductory meeting on June 4, 2009. We then held meetings at which each subcommittee invited experts to provide valuable insights to inform the work of that particular subcommittee. Each subcommittee meeting also began with a special guest who provided context for the day.

Our goal was to provide holistic solutions to the multidimensional challenge of protecting youth online. This was accomplished by building upon the teachings of three task force reports issued over the prior ten years – the COPA Commission report, the "Thornburgh report," and the Harvard University Berkman Center Internet Safety and Technical Task Force report –and hearing from every aspect of the child safety ecosystem. . From the breadth and depth of the 39 recommendations we made in our report, "*Youth Safety on a Living Internet*," I think we succeeded in meeting our goal.

Before I share these specific recommendations, I want to share one concept that became quite clear as a result of this engaging process. As we say in the first line of the report, the Internet is a living thing that reflects at any given moment in time our humanity's lives, sociality, publications and productions. It is very much a part of our lives and similarly our lives are very much a part of it. As such, users online are intertwined with and often responsible for their own safety in this living thing. And given its dynamic nature, there is no one-size-fits-all solution and no silver bullet. Finally, our youth recognize how our offline and online worlds are intricately intertwined far better than we adults do.

It is with full recognition of this moving, living, breathing medium that we make our recommendations.

Instead of repeating the subcommittee reports in its entirety, here are some key recommendations that came from the work of each subcommittee.

The Subcommittee on Internet Safety Education found that applying the Primary/Secondary/Tertiary models used in risk prevention programs would work well in Internet safety programs, especially since a high correlation exists between offline and online risk. Thus, this subcommittee recommended in part that a continually updated online research database is necessary, as is the need to coordinate the multitude of federal government educational efforts in progress.

The Subcommittee on Parental Controls & Child Protection Technology found that a diverse array of protective tools is available today. These tools are most effective as part of a "layered" approach to child online safety especially one that supplements parental education. Thus, this subcommittee recommended that a common set of terms be created to help parents understand the various tools better and that these technologies be 'baked' into online products where possible.

The Subcommittee on Child Pornography Reporting found that the PROTECT Our Children Act of 2008 had made marked improvements in the child pornography reporting process having instant impact on the volume of reports being made by the online industry to the National Center for Missing and Exploited Children. Yet, nascent and smaller service providers need to be brought into the reporting fold. Thus, the subcommittee

recommended that these smaller providers be helped along by the larger industry and work more closely with NCMEC. The subcommittee also recommended the consideration of tax credits for industry given the high development cost of proper reporting and data protection.

Finally, the Subcommittee on Data Retention highlighted the multiple facets to determining what data and how much data should be retained by service providers. Varying viewpoints from the law enforcement, privacy advocacy, and industry sectors were considered. It was clear that law enforcement has a significant need for certain data to properly investigate crimes against children online. It was also clear that this need must be balanced with privacy concerns from legitimate users and the costs of data retention by service providers. Thus, the subcommittee recommended that this discourse be maintained at the federal level to achieve the greatest progress and that Congress take a close look at data preservation procedures enacted through the PROTECT Act before considering mandatory data retention.

These are just some of the 39 recommendations we make in the OSTWG report. Just as we observed that the Internet had evolved from merely a technical tool to a reflection of our living society, we also became markedly aware of what I consider to be 50,000 foot-level achievable recommendations for future Congresses to consider when creating task forces and working groups.

First, provide proper support and funding to task forces and working groups. Unfunded mandates quickly place undue burdens on our citizens who stand ready to serve the American public.

Second, fill the prescription that this and any working group writes by perhaps mandating a group whose sole purpose is to drive execution of the recommendations.

Third, create a cross-functional/cross-agency coordinating body led by the government with members from every sector of the child safety ecosystem to build consensus and coordinate execution efforts.

Fourth, conduct a review of all the online safety related programs the federal government has already undertaken and highlight the most successful ones. These programs can be a great place for public/private partnerships.

Fifth, take a multi-stakeholder approach when solving the complex issues presented by today's new media environment. The OSTWG was successful for exactly this reason.

We in the industry must be a critical part of the solutions as well.

Having led safety efforts at MySpace and News Corporation from the time that the social media industry was just an infant and before that at Microsoft Corporation, I offer you examples of just how the industry can take a holistic approach to online safety. As unusual as it may sound, the industry can find parallel and sometimes exact solutions to online challenges in the real world. Every online safety program must consist of technology, education, collaboration and enforcement designed to prevent unwanted content, contact and conduct.

As builders of these technological platforms, industry must provide both front end user tools and back end member protections. MySpace, for example, provides users the ability to block anyone from contacting them, reducing incidents of cyberbullying. MySpace also automatically locks an account that appears to have anomalous activity to prevent phishing and spam attacks against users.

The best technical solutions must then be coupled with educational programs to raise awareness about healthy online behaviors. MySpace provides guides for parents, teens and school officials with exactly this purpose. The school guides have reached over 55,000 schools in this country. MySpace also uses teachable moments

across the site such as during the photo posting process where users are informed about acceptable content policies.

While industry may be expert in technology, we must collaborate with experts in other sectors of child online safety. MySpace has formed relationships with the National Center for Missing and Exploited Children, iKeepSafe, Connect Safely, and Enough is Enough – some of the leading child advocacy organizations in the country. Working with NCMEC, MySpace sends AMBER Alerts to users when a child is kidnapped or missing. MySpace also works with the National Suicide Prevention Lifeline when a user is in crisis to get them help immediately thereby preventing possible suicides.

At the end of the day, we know that illegal incidents can occur, thus working closely with law enforcement 24/7/365 is a must for all of us. MySpace works with law enforcement to respond to requests for information that might help bring a perpetrator to justice. MySpace also works with law enforcement directly to assist in runaway situations in an effort to reunite runaway teens with their families.

Thus, any industry online safety program must be holistic in nature encompassing technology, education, collaboration, and enforcement. I will say that the industry has come a long way since my own days as a child predator prosecutor in the Department of Justice.

Speaking more broadly, as this subcommittee examines Protecting Youths in an Online World, you have a significant and undeniably critical role to play that we in the industry would embrace with open arms and one that is necessary for the protection of this nation's children online.

> Convene the Experts to inspire the dialogue. Today's hearing is a great example of just this. The more places that you can inspire folks to gather, discuss, and analyze, the more pointed solutions can be identified.
>
> Educate the Masses to increase safer online practices. The more we can mandate educational programs at every level of our education system, including colleges, the healthier our citizens will be in their daily online practices.
>
> Fund the Programs to implement safety solutions. A perfect solution to a complex problem without proper funding is no solution at all. This is very much like recommending that students learn to read in elementary school without providing teachers and books to make that happen.

I look forward to working with this subcommittee to identify specific action items that can help you convene the experts, educate the masses and fund the programs.

In closing, I think we can step forward fully cognizant of the challenges that lie before us in protecting youth online and at the same time greatly hopeful that we can find and implement solutions that will allow our children to grow up healthy in this digital age.

Thank you Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee for giving me this opportunity address you.

Hemanshu (Hemu) Nigam | Founder | SSP Blue

Hemanshu (Hemu) Nigam is the founder of SSP Blue, the leading advisory firm for online safety, security, and privacy challenges facing corporations and governments. A veteran of online security, he brings over 20 years of experience in private industry, government, and law enforcement. He has been called upon by institutions from the United Nations to The White House to provide counsel on the world's most critical online protection challenges and has been a featured expert by BBC, *BusinessWeek,* CNN, *Financial Times,* Fox News, *The New York Times*, and *The Wall Street Journal*.

From 2006 to 2010, Hemu was Chief Security Officer for News Corporation's numerous online properties, responsible for protecting the personal information of over 200 million users around the world. He has been credited with making MySpace safe and secure after launching initiatives like Sentinel SAFE, technology to identify and remove criminals from the social networking site. He also drove the launch of over 150 other safety, security, and privacy protection features for MySpace and played a key role in an accord between MySpace and 49 State Attorneys General to develop key principles of social networking safety.

Previously, from 2002 to 2006, Hemu worked for Microsoft where he led a global initiative to build safety standards into products across the company from Xbox to MSN to Windows. He also implemented a virus enforcement strategy and collaborated with the U.S. Secret Service, Interpol, and the FBI to develop Microsoft's landmark Anti-Virus Reward Program. The program is credited with toppling one of the world's most notorious virus creators in 2005.

From 2000 to 2002, Hemu was Vice President of Worldwide Internet Enforcement at the Motion Picture Association of America, where he spearheaded a global effort to combat online movie piracy for the major Hollywood studios. During his tenure, Hemu implemented anti-piracy technology that allowed MPAA to eliminate more than 100,000 illegal movie websites in a year.

From 1997 to 2000, Hemu held simultaneous roles in the federal government, serving as a federal prosecutor against child and computer crimes for the U.S. Department of Justice, advisor to a Congressional commission on child safety, and advisor to The White House on cyberstalking. In addition to prosecuting Internet predators, Hemu was behind the prosecution of 17 foreign nationals engaged in the trafficking of women and children into the United States.

Hemu began his career as a deputy district attorney in Los Angeles County from 1990 to 1997, specializing in prosecuting sexual assault and child abuse cases. During his tenure, Hemu handled over 1,000 criminal matters and was a recurring lecturer at rape crisis centers across Los Angeles.

Hemu recently worked with Harvard University's Berkman Center for Internet & Society and the State Attorneys General to develop widely used online safety standards. He currently serves as co-chair of President Obama's Online Safety Technology Working Group and sits on the board of the National Center for Missing and Exploited Children.

He earned his juris doctorate from Boston University School of Law and his bachelor's degree in government and political theory from Wesleyan University.

###