PREPARED STATEMENT OF HEMANSHU NIGAM
FOUNDER AND CEO, SSP BLUE

"PROTECTING CHILDREN'S PRIVACY IN AN ELECTRONIC WORLD"

THE SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE OF THE HOUSE ENERGY AND COMMERCE COMMITTEE

UNITED STATES HOUSE OF REPRESENTATIVES
2123 Rayburn House Office Building

Washington, D.C.
October 5, 2011

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, thank you for giving me the honor of appearing before you today to provide insight on the best ways to protect children's privacy in an electronic world.

I have been at the forefront of nearly every major aspect of offline and online child safety for the past 20 years. Today, I am the founder and CEO of SSP Blue, a safety, security, and privacy strategic business consulting firm for online businesses. My company provides clients with strategic guidance on creating an online presence that protects their consumers, promotes corporate social responsibility, and engages in partnerships with government, law enforcement, and NGOs. Past and current clients have included News Corporation, Microsoft, AT&T, Tagged, Formspring, and others. To be clear, I do not speak on behalf of any of our existing or past clients.

Prior to SSP Blue, I served as News Corporation and MySpace's Chief Security Officer when social media was barely a toddler. Prior to that, I worked inside Microsoft Corporation to set in motion a cross-company strategy for child safe computing and led a cyber security enforcement

team. Before Microsoft, 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, and as a father of four children ranging in age from 6 to 16.

I want to first praise the work of the Federal Trade Commission for its meticulous and thoughtful approach in reviewing the Child Online Privacy Protection Act ("COPPA") to identify areas of improvement.

As a backdrop, I also want to stress a concept easily forgotten. The industry has an incentive to do the right thing when it comes to protecting children's privacy rights. Businesses lose when they are accused of violating a child's rights – their brand reputation suffers, their consumer loyalty drops, their friends in child advocacy groups disappear, and most important, they lose the trust of the parents and guardians who care for the very children they cater to. In essence, doing the right thing is synergistic with the short and long-term viability of a business – with survival.

Within this context, I would like to provide this Subcommittee a framework on how we should approach whether changes are needed in COPPA and what they should be.

Whenever we think of protecting children, whether it is for their safety, security, or privacy, our first inclination is to protect them from anything that sounds 'bad' instead of just what is 'bad'. Solutions based on things that sound bad eventually fail. In the past ten years, I've had the honor

of advising the COPA Commission, sitting on the Berkman Center Internet Safety Technical Task Force, and co-chairing the Online Safety Working Group. In each endeavor, we could have taken the easy way out by offering a myriad of solutions in response to problems that sounded bad. Instead, we focused on identifying whether and what the problem is that we needed to solve. Only then did we articulate necessary solutions.

While technologies may have evolved since the advent of COPPA, I urge you to consider whether an actual problem has been clearly articulated that needs to be solved when looking at each individual change that is being proposed.

Next consider whether existing regulations can be used to respond to an identified problem. Looking back on the FTC's COPPA enforcement actions, it is clear that current regulations have been quite useful and effective. In fact, a great majority of the industry does a tremendous job in working within the framework and guidelines whether their product is directed at minors under 13 or 13 and over. Even new companies know what is expected of them before they enter the marketplace. Interestingly, companies find providing services to 13 plus a much better business model.

We must ask whether there are today other bad actors that the FTC finds it cannot enforce against. Has the evolving landscape created gaps? In some areas the answer is yes and in some areas perhaps no.

In areas where existing regulations needed to be adjusted, we should then determine what the best solution would be. Several factors will affect the outcome. We must ask whether the proposed change:

1. would actually close an identified gap

2. create technical implementation challenges especially given the multitude of products and business models that often exist inside a single company
3. lead to conflicts with other agency and department demands or expectations that are just as legitimate such as the conflict that arises between date retention, minimization, and preservation, or
4. lead to unintended consequences such as creating disincentives to providing rich online experiences for the under 13 members of our digital society.

If we can utilize this framework when considering the proposed changes, I think we will be able to protect our children's privacy by implementing solutions that work in an ever evolving interconnected world.

I do want stress that if we are to accept all the changes proposed, we can expect an immediate impact on the marketplace:

1. Larger companies will try to adjust to the changes, implementing fixes where they can and shutting off areas where too much uncertainty lies;
2. Smaller Companies seeking venture capital investments will find it harder to obtain funding in the face of unclear paths to defendable implementations.

That said, as with any new regulations, once they are tested and clarified, the industry will eventually feel more confident to invest again. But, such a cycle can be avoided if we spend the time to examine the proposals within the framework I have outlined above.

In closing, I want to stress the importance of protecting children's privacy in today's electronic world. Our task is to do it in a way that responds to clearly identified problems with effective

solutions that can be properly implemented by those who are already incentivized to do the right thing.

Thank you Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee for giving me this opportunity to address you on this important topic.

////