

Opening Remarks by Stephen Balkam, CEO, Family Online Safety Institute

So, here we are. We meet at a most remarkable time. We are at the mid-way point in a shift from one US Administration to another. It is no exaggeration to say that the eyes of the world are watching every signal that emerges from the Obama transition team and members of the new Congress.

And we, in the online safety world, are keen to hear what plans they may have that will impact our work, in this country and beyond. We are just as keen to communicate our thoughts and proposals in order to positively impact the debate on how best to protect our kids while also respecting free expression.

And so this would be a good time to rethink and reframe what we do, say and teach about “online safety”. Is the term itself, obsolete? Does it conjure up an image of fear, of bad men out to lure and molest our innocent children? Are we still stuck in a Web 1.0 way of thinking that portrays our children as passive “victims” and the net as a scary place of pedophiles, perverts and pornographers?

Yes, there are predators on the web. And, yes, the ease of access to adult material continues to create real problems – not least in the pornification of our society and the early sexualization of our children. We have yet to see what the full impact of freely available online porn will have on this generation of young adults.

But do programs such as To Catch a Predator accurately portray what is really going on? Does a televised sting operation in unmoderated chat rooms really reflect the realities of a Web 2.0 world of YouTube, MySpace, Facebook and Club Penguin?

Or does it say more about how some in the media have exploited the fears of parents and policy makers and how that fear has permeated how we craft laws and teach our kids how to stay safe?

At this extraordinary time of transition, it’s time to move from one paradigm to another: from a Web 1.0, fear-based approach to a more Web 2.0, fact-based model, one that is fully grounded in research of actual harms and actual behaviors of children and teens.

I am delighted that we have some of the leading academic researchers in the world with us today who have studied the many and various problematic issues created by our always-on, permanently connected kids. Let’s pay special attention to them and what they have to say. And, needless to say, much more research is needed in this fledgling field.

Let’s move away from fear-mongering and talk more about conveying to every child a sense of digital citizenship. Yes, let’s teach them the basics of online stranger danger, but let’s also convey to them the knowledge, skills and values they’ll need to make wise and safe choices online.

And let’s recognize that for a small percentage of teens, those who are at-risk in the offline world, that they will be the ones most at-risk online. These are the teens – boys and girls – who will act out and seek out dangerous and risky situations and who knowingly go to meet strangers they’ve met online for sex or risky thrills.

For these kids, we need effective risk prevention approaches – targeted and directed – not a scattershot approach that assumes all kids and teens are in imminent danger of being abducted or sexually abused.

We need to re-think online safety education messages and methods to achieve these two quite distinct goals.

We need to engage psychologists, social workers and mental health practitioners and merge the fruits of their thinking and experience into the creation of online safety tools and educational programs.

At last year's conference I announced that in 2008 we would look at existing education efforts provided by industry, government and the nonprofit sectors here in the US. In addition, we committed to holding Roundtable discussions to bring in experts from the three sectors to challenge the status quo and to propose a range of ideas and programs for future action.

The result of that work, Making Wise Choices Online, is published today and I commend it to you – it is in your bag which we gave you as you came in and we have posted it on our website today.

In it you will find a summary of the discussions we held here in DC in the Spring, in Oxford, England in the summer and at Google's campus in September. In addition, you will find detailed grids of most of the prominent online safety education and training programs.

These grids, which we have entitled, US Online Safety Education Initiatives have been added to FOSI's website today and will be constantly updated as we learn of more efforts.

These roundtable discussions helped to illustrate the vital importance of what we call the 6 layers and the 3 C's of online safety. That is, for us to create a safe, healthy and productive environment for our kids, we need the following six layers to work in tandem:

- Reasonable government oversight and support
- Fully resourced law enforcement
- Robust and comprehensive industry self-regulation
- Tech-savvy teachers
- Empowered parents and
- Resilient kids making wise choices about the:

Content they access and post online

Who they contact and who they allow to contact them

And how they conduct themselves online

In the past 2 months, the US Congress has passed two bills that qualify as "reasonable oversight and support".

Before he left office, Senator Stevens saw into law his bill which asks the FTC to conduct national awareness raising and educational initiatives; the schools that receive the e-rate to include online safety in their curriculum and for the NTIA within the Department of Commerce to create a Working Group to explore the state of tools and rules to keep kids safe online.

Senator Pryor's recent bill requires the FCC to conduct research into "advanced blocking technologies" for use on the Internet. Some have described this measure as laying the groundwork for a V-chip for the

Internet. While we welcome these new initiatives, we will also keep a watchful eye on any move to mandate or chose a technology winner.

If you add in the programs being undertaken by the Departments of Justice and Education, we now have five parts of the federal government with varying degrees of responsibility for this issue. What is lacking is any high level co-ordination and leadership.

Which brings me to the four recommendations to the new Obama Administration we list in our report today.

First, we propose an Annual White House Online Safety Summit, convened by the President, that brings together the relevant government departments, industry and nonprofit leaders to review progress and set goals for the coming year on a range of online safety measures. This is similar to what has been established in the UK following the Byron Review and what the Clinton Administration hosted in the late 1990s.

An annual summit will provide an ideal opportunity for the President to use his bully pulpit to exhort everyone to do more to protect kids online and to create a national dialogue within the media that will carry over to the next annual event.

Next we propose the creation of a US Council for Internet Safety (USCIS) that consists of heads of relevant government departments, industry leaders and NGO representatives. The Council would be responsible for creating a national strategy on online safety and for overseeing its implementation.

The Council would provide an important forum for regular dialogue across sectors and between government departments to maintain a focus and impetus behind the agreed upon initiatives.

Thirdly we propose a \$100M Online Safety Program to fund a range of educational and awareness raising projects. It would also pay for research and the evaluation of the effectiveness of existing and new projects funded under the program.

This proposal borrows heavily from the EU Safer Internet Program model and would create a much needed pool of resources for peer-reviewed, academic research into the many and complex online safety issues emerging in a Web 2.0 world.

And, finally, we propose the creation of the post of National Safety Officer within the office of the new CTO as currently proposed by President-Elect Obama. This officer's responsibility would be to work with the US Council for Internet Safety, oversee the Online Safety Program and be the point person within the Administration for all aspects of online safety. This post would pull together all the many and varied government efforts and programs that are currently spread over a half dozen departments and agencies and provide much-needed coherence to the nation's response to this issue.

Today we have sent these proposals to members of the Obama Transition Team and we look forward to their response.

For our part, we have already begun planning for a joint event with CTIA, The Wireless Foundation for an event in the Spring here in DC, with the GSM Association in London in June and we are in talks with France Telecom for a September event in Paris.

And, of course, we hope you will return for our third annual conference here in DC, which we will pull back into mid-November next year.

We look forward to working with each of you on these and other initiatives that will help to create this new paradigm of online safety, one that is based in new, ground-breaking research, innovative techniques and tools and a new way of talking with our children.

With this shift, this transition, our kids will truly be safe at any speed, provided we give them the tools, the rules and craft the supportive public policies to keep them that way.

Thank you

Keynote Address by Hemanshu Nigam, Chief Security Officer, MySpace

Good Morning. Thank you, Stephen and the Family Online Safety Institute for hosting this event. Stephen, it is an honor to share the stage with you today -- the work you and your organization do is an essential component of the industry's effort to increase the online safety of today's youth. And, thank you to my industry colleagues who are here and who have worked over the years in a joint effort to achieve online safety. I also want to acknowledge Attorney General Roy Cooper who is with us today. Since I joined MySpace, I've developed a close relationship with General Cooper and his office. We thank him for all that he has done to protect North Carolina's children and this nation's children.

MySpace and other social networking sites have been a great innovation for all Americans, regardless of their age. Our sites allow users to share their interests and make new friends. Our goal is to nurture and expand this community, while providing for a safer online experience.

When Fox Interactive Media and News Corp., acquired MySpace in 2005, we had 22 million registered users. A year later, that number grew to 90 million. Today, we have nearly 118 million monthly active users spanning 30 countries, in 15 languages around the globe.

To put it in perspective, 1 in 4 Americans are on MySpace.

This amazing growth has created many opportunities as well as challenges for us. We often talk about the virtual world of the Internet as separate and apart from everyday life. However, as our teens spend more and more time online this has become a difference without a distinction. Rather than treating the online and offline worlds differently, our goal has been and will continue to be to make our virtual neighborhoods as safe as our real ones.

Providing a safe place for members is the right thing to do. It also makes good business sense. Our members deserve a safe place within which they can freely connect and explore. Our advertisers demand the safest possible site within which to promote their brands. We simply have to make this possible.

In 2006, I joined MySpace as its first Chief Security Officer. My job at MySpace is to provide a safe and well-lit community for all our members. For the past 18 years, I have led efforts to find online safety solutions. Before coming to MySpace, I set in motion a cross company strategy for child safe computing and led a cyber enforcement team at Microsoft. Prior to that, I was the first Vice President of Worldwide Internet Enforcement at the Motion Picture Association of America. I also served as a prosecutor

against Internet child exploitation at the US Department of Justice, and advisor to the COPA Commission as well as the Vice President's Committee on Cyberstalking. Finally, I worked as a prosecutor in the LA County District Attorney's office, specializing in child molestation and sex crimes cases.

This work is my passion, and has been my personal commitment for the last 18 years. The leadership at MySpace, Fox, and News Corporation gave me a simple mandate – Bring the company to the forefront of online safety efforts in the social networking industry.
(The MySpace online safety framework)

In order to make progress in a short period of time, we needed a concrete framework to guide our efforts in online safety and security. There are several important elements of this framework that have directed our progress over the last two years and that continue to guide us everyday.

These include:

- Protecting teens from unwanted contact
- Preventing teens from access to inappropriate content
- Providing tools and education for parents and teens to protect themselves
- And finally, partnering with law enforcement agencies, safety advocates, and NGO's globally

Our online safety framework has been very successful in the last two years. In fact, we have already implemented over 100 safety features and programs designed to increase user safety.

A great example of how our efforts to build the safest social networking site in the industry are working occurred a few months ago. I was speaking at an Internet youth marketing conference in San Francisco called YPulse. When a member of the audience, who is starting her own social network, asked me the following: "We are a small company—she said, and we need to know which safety elements our site must have in place to be safe?"

The answer to this question embraces what we at MySpace like to call the "Big Six" – safety elements that every social networking site must have in place as a minimum bar to entry and all of which should be adopted on an industry-wide basis. Only by implementing the Big Six, can sites adequately protect their users, particularly teen users, from dangers online.

Let's take a walk through The Big Six –

- First: Image and video review. Sites must find ways to review hosted images and videos, deleting inappropriate ones when found. At MySpace, we proactively review these hosted image and video for inappropriate content like pornography and extreme violence, using a combination of humans and technology. We then digitally fingerprint the banned images to prevent them from being uploaded again. If we can do this with nearly 20M uploads a day, others can too.

- Second: Discussion groups review. Social networking sites must review discussion groups to find harmful subject matter, hate speech, and illegal behavior, deleting that content when it is found. MySpace reviews such groups and we are building new technology to enhance our abilities in this area.

- Third: Removing registered sex offenders. Social networking sites must ban registered sex offenders from setting up accounts on their sites using technology that already exists today. In a moment, I'll talk about the one we helped develop for the industry.

- Fourth: Meaningful efforts to enforce minimum age requirements. Sites must enforce their minimum age requirements and take steps to identify and remove underage users who have misrepresented their age to gain access. MySpace utilizes a combination of human review and automated programs to find and delete underage users, and we are continuing to improve these tools.

- Fifth: Protection for younger users from uninvited communication. Social networking sites must implement default privacy settings that prevent adults from contacting teens under 16 who they don't already know in the physical world. Adult MySpace users cannot contact 13, 14 and 15 year old users if they don't know their last name and email address, information not available to users of the site. MySpace makes these privacy settings available to all of our users, regardless of age.

- Sixth and Finally: Collaboration with law enforcement and online safety advocates. All sites should have law enforcement hotlines available at all times to assist law them during emergencies and non-emergencies and should also partner with online safety advocates to increase awareness and education about online safety practices. MySpace has set up a dedicated 24/7 hotline and email address to provide assistance to police whenever they call. We also work with law enforcement in a variety of ways, from educating cybercrime units to providing educational materials on the best way to work with us. So far we've trained over 4,000 cops in person. MySpace has also created partnerships with iKeepSafe, Enough is Enough, and The National Center to create social networking safety training tutorials and other educational materials for parents, teens, and educators. We continue to look for new avenues to raise awareness.

MySpace has also been part of the industry-wide Internet Safety Technical Task Force that was established earlier this year to research and develop online safety tools that can help make users safer and more secure. The formation of this Task Force was a result of the "Joint Statement" that MySpace adopted at the beginning of the year with fifty Attorneys General with the goal of establishing key criteria to set the internet safety bar. Headed by the Berkman Center for Internet Society at Harvard Law School, the Task Force includes members from the corporate, technology, and non-profit worlds. In addition to MySpace, it includes industry leaders like AOL, Comcast, Google, Microsoft, Verizon and Yahoo!, as well as FOSI, The National Center, iKeepSafe.org, Enough is Enough, and Connect Safely.

This unprecedented Task Force was given the unique and challenging mandate to produce a Final Report that provides industry wide internet safety recommendations based on the findings of the Research Advisory Board and Technical Advisory Board. Comprised of leading researchers in the field, the Research Advisory Board conducted a comprehensive Literature Review of all published research on the true risks minors face online. And the Technical Advisory Board, comprised of a range of technology experts, solicited and reviewed submissions from available technology vendors and reported back to the Task Force on its findings.

The highly anticipated Final Report is slated to be released within days. The Report will reflect the state of current online safety technologies and will identify key areas that industry, NGO's, and government can focus their efforts on to further increase online safety. As a founding member of the Task Force, we are excited by what we learned and the call to action that will come from these learnings.

Additionally, and for the benefit of my colleagues who are here today from across the pond, I want to highlight that we are also part of the European Union Social Networking Taskforce. This task force is dedicated to bringing together key stakeholders to develop a pan European code of conduct to protect

minors on social networking sites. This has come from work that has been done in the UK on the Social Networking Guidelines and by Dr. Byron who joins us here today. Needless to say MySpace is proud to be a part of this global effort to increase online safety.

As I mentioned in the Big Six, MySpace blocks registered sex offenders from our site. Perhaps our most important innovation is Sentinel SAFE, a national searchable database that MySpace developed in partnership with Sentinel Tech. This database, the only one of its kind, contains information on the estimated 600,000 registered sex offenders in the U.S. Our team uses Sentinel SAFE to help keep these predators off of our site, and we provide the information to Attorneys General in all 50 states.

However, our effort to remove registered sex offenders would be even more effective if we required convicted sex offenders to register their online addresses in the same way they are currently required to register their physical addresses. That way, if they don't follow this law, they get a ticket back to jail, just like they do in the physical world.

Twenty-one states have already enacted this legislation and many others will have the law pending in their legislatures this coming year.

We have also supported similar legislation at the federal level. In fact, the KIDS Act was just recently passed and signed into law by the president. The KIDS Act was originally introduced by a bipartisan, bicameral Congressional delegation after consultation with MySpace. The new law requires convicted sex offenders to register their email and instant message addresses with the National Sex Offender Registry. MySpace and other social networking sites can then use this information to keep registered sex offenders out of their social networks.

We look forward to a day when every state has this law in place to assist law enforcement and to better allow companies like ours to quickly identify and block sex offenders from membership.

Additionally, MySpace supports legislation that would increase penalties for predators online. We also support increased resources for law enforcement in order to investigate and prevent these crimes, and for education and awareness programs directed at teens and parents. We as a country must do even more to direct sufficient resources against cybercrime. MySpace is working hard to draw attention to these challenges and to help find solutions at the state, federal and international levels.

We also believe that the industry should focus on the need for education and tools for parents, educators and teens. We provide extensive educational resources on our site, including access to our safety site found at: myspace.com/safety as well as links to safety tips on the bottom of every page of our site.

Earlier this year we joined with iKeepSafe to release a broadcast PSA titled "Don't Stop the Dialogue" that aired on all FOX broadcast and cable networks reaching over 150 million viewers. The PSA was geared to encourage parents to talk with teens about their Internet use and help them to be safer online. Parents are equipped with the know-how and ability to talk with their teens about appropriate and safe behavior. They simply need to extend these conversations to online activities.

MySpace has come a long way in the last two years. We've seen an explosion in the number of users on our site. We've experienced tremendous demands on our infrastructure. And, we've overcome many challenges to manage this revolution.

We've been able to implement these changes under the weight of nearly 118 million monthly active users around the globe. So, if we can do it, any company, of any size, can do so as well. Our mission to improve online safety is part of a continued effort to create an industry transformation. It is time for a paradigm shift. It is time to move beyond the days of just notice and takedown, to a day when we proactively find solutions to protect all of our users.

And so, I firmly believe that the same kind of progress can be made by every member of our industry. The Big Six elements we pioneered must be adopted.

And if all of us step up and do our part, the future for us is a bright one.

I can see a day when the online world is full of clear and articulate expectations –

- A day when law and policy makers know what they should expect from a new company entering the digital age
- A day when parents are better empowered to know just how to raise their teens in an ever connected digital world
- A day when companies know the types of programs, technologies, and safety features they must implement online in this digital century

Every company, every policy maker, every NGO, every educator, and every parent needs to know – the bar has been set.

Thank you.

Remarks from FCC Commissioner Deborah Taylor Tate

Good Morning. Thank you to Mr. Stephen Balkam, not only for including me in this important day, but for your continued commitment to our children's safety. And thank you, Mr. Hemanshu Nigam, for those thought-provoking words. As a former federal prosecutor you know perhaps better than anyone here the type of perilous threats that our children face every time they log on. Thank you for committing to make MySpace part of the community of innovative, forward-thinking problem-solvers assembled here today.

Most of you know that I have dedicated my career to improving the lives of children and families. I have championed issues from childhood obesity to family-friendly programming, and of course increasingly regarding internet safety. Thank you to the corporate representatives, associations, stakeholders, software developers, ISPs, academics, and all the stakeholders gathered here today. I applaud your commitment and encourage even more self-regulatory and voluntary online child safety efforts, rather than heavy-handed government regulation.

I. Progress in U.S.

We have made a great deal of progress in the U.S. over the past few years. In New York, Attorney General Cuomo has launched an historic agreement with ISPs such as AT&T, Verizon, Comcast, AOL, and Time Warner to block access to websites and Newsgroups containing images of child pornography. This is a partnership with the National Center for Missing and Exploited Children (NCMEC), which will provide a list of web addresses where child porn is found. Every major ISP in the country has signed this agreement. In California, Attorney General Jerry Brown and Governor Schwarzenegger have called for similar action by that state's ISPs. Other states are also making great strides. Last week, I received a call

from a state senator in Missouri who was in D.C. participating in the American Legislative Exchange Program. That group is getting involved at the state level. I encourage cooperation at all levels of government.

II. Partners

FOSI continues to be a leader in the online safety arena, taking yet another step this week with the release of their report “Making Wise Choices Online.” I strongly support the four initiatives recommended in this report, especially the idea of an annual White House summit— and why just one? Why not a series all across the country? I also support the creation of a permanent U.S. Council for Internet Safety. I stand ready to partner with you in these efforts and lend my support today and in the future.

Ikeepsafe is another leading partner in the effort to protect children online. Ikeepsafe has developed “Faux Paw the Techno Cat,” a series of educational materials designed for elementary school children that offer entertaining and informational messages about the importance of internet safety. The curriculum is being used internationally and has been translated into Spanish, French, Mandarin, Cambodian, and Vietnamese.

Corporate partners are also emerging, with AT&T, Verizon, MySpace, Sprint, Microsoft, Comcast, Charter, Cox, and today’s sponsors and exhibitors—many of whom are offering parental tools and educational materials to help parents keep their children safe online.

III. Government

Many Members of Congress have made internet safety a priority as well. Just last month, the Child Safe Viewing Act, sponsored by Senator Pryor, was signed into law. That bill will require the FCC, within 270 days, to study and report on the various blocking technologies available on wired, wireless, and Internet platforms.

In October, the President signed another bill sponsored by Senators Schumer and Stevens that will direct the Attorney General to: (1) require sex offenders to provide to the National Sex Offender Registry all Internet identifiers, such as email addresses, and (2) specify requirements for keeping Internet identifier information current.

Another idea I have championed during my three years at the Commission is tying e-rate funds to internet safety education. I believe that schools that receive e-rate funds should be required to dedicate a portion of their online curriculum to teaching students about cybersecurity. Thus, I was thrilled to see the President sign the Protecting Children in the 21st Century Act. That bill, originally introduced by Senator Stevens, requires schools receiving e-rate funds to offer education regarding online behavior, including social networking, chatrooms and cyberbullying awareness and response; directs CTIA to create an interagency working group to identify and encourage technologies and initiatives to help parents protect their children from unwanted content; and requires a national public awareness campaign to be conducted by the Federal Trade Commission.

IV. International

While remaining mindful that we are often a benchmark in the information and technology space for the rest of the world, we should also remember that all the answers are not in Washington, and we should consider innovative and successful steps other nations are taking to protect children online. In the UK, Prime Minister Brown as one of his early initiatives, commissioned a study, by Dr. Tanya Byron,

regarding the risks to children from exposure to harmful or inappropriate content online. I truly enjoyed being interviewed by Dr. Byron, and one of the key findings from Dr. Byron's study is what I have termed the "new digital divide." That is the generational, rather than economic, digital divide that results as parents feel increasingly ill-equipped to keep up with technology and therefore ill-equipped to truly protect their children cyberspace. While many of us in developed countries may be ill-equipped or even over-whelmed, think about those parents in nations that do not blog or shop or research online. In fact, many parents have never utilized a computer- or a cell phone for that matter- or even more problematic, those parents that are functionally illiterate.

In Japan, DOCOMO, the largest wireless provider, has developed a curriculum and actually sends instructors into schools to train children on the importance of internet safety. The curriculum is broken down into three parts: 1. basic rules and manners, 2. how to deal with SPAM (filtering service, etc.), and 3. abuse and slander on the internet bulletin boards, blogs, and profiles. As of July 2008, DOCOMO had attended 6120 classes and interacted with 1 million students.

Many developing nations are on the cusp of an explosion in broadband deployment—and the children in those nations will need the same type of cybersecurity training—although many times woefully inadequate-- our children receive or have access to. I have been pleased to literally spread the word regarding child internet safety all around the world. Last month, I was honored to participate in the launch of the Child Online Protection Initiative (COPI) at the High-Level Segment of ITU in Geneva, Switzerland, led by Secretary General Hamadoun Touré. I hope that all of you, and your companies and associations, will support this initiative and make your organizations' tools and resources available for use by providing them to COPI. This is not just an issue for America's children, but now extends to the world's children.

V. Other Initiatives

Let me mention and applaud the work by our sister organization, the FTC and recognize my colleague Commissioner Pamela Jones Harbour for their website "OnGuard Online" – which provides practical tips regarding internet safety and security. They also provide "You Are Here," an interactive online game for youth that teaches everything from false advertising to target marketing; again as our worlds collide, we must protect our children in the online world just as we do everyday in the offline one.

VI. Conclusion

The Internet and broadband have literally brought the world to our children, and as technologies converge, the opportunities are endless. They must be part of this on-going dialogue as well. We need not only teen-to-teen outreach, but also their help in reaching even younger generations of new internet users. However, as we have seen, these dazzling innovations and life-changing services also pose risks— to all of us, however, most importantly, to our children. In order to ensure that the next generation reaches their greatest potential, we must ensure that they have access to a wealth of educational information in an environment that protects their personal information, physical safety, and healthy mental development.

Thank you for the opportunity to participate in this event. I know you all share my goal of first and foremost continuing toward our national objective of broadband deployment for all our citizens, no matter where they choose to live. Using all of our joint resources and synergies will enable the vast benefits of information and communication technologies to be available in the safest environment for children here and around the globe. I look forward to working with you in the future, whether as Commissioner Tate or Citizen Tate. Thank you.