REMARKS OF COMMISSIONER DEBORAH TAYLOR TATE AT ITU COUNCIL, GENEVA, SWITZERLAND "BE SAFE ONLINE: A CALL TO ACTION" 13 November 2008

Mr. Secretary-General, Excellencies, Distinguished Delegates, and honored guests, thank you for inviting me to be here. It is an honor and a privilege to appear before High Level Segment of the 2008 Session of ITU Council. This session, the first international-level convocation of its kind to focus on an issue of critical importance to all of us, would never have occurred without the vision and leadership of a world leader – but, more importantly, a father of four, and grandfather of two-- Secretary-General Dr. Hamadoun Touré. Dr. Touré has provided leadership and advanced online safety as an international issue. On October 7, Dr. Touré launched the Child Online Protection Initiative, recognizing that, in his words, "the online world respects neither boundaries nor borders."

Hand in hand with our collective desire and our individual national focus on the deployment of broadband, comes the realization that we must recognize both the vast opportunities the internet offers—from economic to e-learning to e-health—and just as important are the risks and very real dangers which this viral and sometimes toxic connection allows. It's been nearly twenty years since Tim Berners-Lee invented the World Wide Web in 1989. This year, at the beginning of 2008, there were 1.3 billion Internet users worldwide—more than three times the total number of people who live in the United States. Brazil has 6.8 million broadband connections; Mexico has 5 million; Viet Nam has 1.3 million; China has 66.4 million; Canada has 9.2 million, and

here in Switzerland there are 2.5 million. Even small, developing nations are making progress. I was recently in Ghana, participating in the West Africa Roadmap to Opportunities Conference, which focused on market development and specifically cross-border cooperation in wireless technology; Ghana is up to over 14,000 broadband connections.

I am not here today representing the entire U.S. government. Rather I am here as one federal official who cares deeply about our children. The U.S. government consists of hundreds of offices, agencies, and departments—from law enforcement, which I will discuss later, to the legislature, to the various administrative agencies, in addition to the Federal Communications Commission. Issues of cybersecurity touch every facet of our government. I have worked as an official at both the state and federal level, and throughout my professional career, my focus has always been on finding ways to improve the lives of children—both in America and around the world. Whether through encouraging childhood immunizations, fighting to end childhood obesity, or promoting more positive content in the media, I believe that the next generation is depending on us to prepare a safe and steady path for them to travel into adulthood.

My goal today is not to speak, but to listen. I want to hear what your nations are doing to protect children from dangers online—and what industry initiatives have seen success. I believe that together we can develop real-world solutions, forge new partnerships, engage relevant industry leaders, and truly find new ways to provide our

children with all of the resources the Internet has to offer, in an environment that protects their physical, mental, and emotional well-being.

I. Scope of the Problem

When we speak about the "digital divide," we recognize that there is a considerable difference in the way our generation perceives the internet, and the way our children do. Like many parents, I never really thought past the benefits the Internet offers – from research for homework, to the wonders of telemedicine, to distance learning opportunities, to creating and producing your own content online. However, we must also realize that this technological explosion of access also presents challenges and very real dangers.

I often remind parents that the internet is no longer just an infrequently-accessed research tool, but a ubiquitous aspect of our children's daily lives. They live in a digital world. As the ITU's website states: in industrialized nations, up to 60% of children and teenagers use online chatrooms regularly and evidence suggests that as many of three-quarters of these may be willing to share personal information in exchange for online goods and services. An entirely new language has developed out of this explosion of technology—we "IM", "blog", "friend" people on Facebook, and use "twitter" to stay in touch with acquaintances. Children participate in chatrooms, post and read messages in social networking sites, and join in online activities such as games.

For those of you representing nations that have little research on the scope of internet usage, let me share a few statistics from the U.S.: A 2007 study showed that 28% of online teens have created their own blog. Twenty-seven maintain their own webpage. Thirty-nine percent share their own artwork, photos, stories or videos online. Forty-one percent of teens who use MySpace, Facebook, or other social networking sites send messages to their friends everyday through these sites — double their e-mails. Today's U.S. college students grew up with the internet—20% began using the internet between the ages of 5 and 8. Seventy-three percent of students say they use the internet more than the library.

With the explosion of educational resources available online, one might think parents would be 100% pleased with the internet's role in their children's lives. But surveys show just the opposite: a late 2006 survey that showed 59% of parents think the internet has been a totally positive influence in their children's lives--- down from 67% in 2004. You might find it alarming that one of the top reasons for college dropouts in the U.S. is online gaming addiction—such as World of Warcraft—which is played by 11 million individuals worldwide.

Even more concerning, the threat is no longer contained to the family computer. It is in the palm of your child's hand. Given the fact that approximately 60% of American teens have a cell phone, and that cell phones are being marketed to children as young as six, I have, and will continue to, challenge U.S. telecom carriers to adopt initiatives to provide curriculum and education regarding safe use of their products—

including internet safety, and the prevention of access to inappropriate websites by children.

II. Dangers and Law Enforcement

A. Predators

One of the major networks in the U.S. recently produced a series of shows called "To Catch a Predator." I was shocked by not only the number of predators stalking children online-- every second of the day—but also their frightening persistence. In the U.S., the statistics range from 1 in 7 to 1 in 25 children who have been solicited online. Four percent of American children have been aggressively solicited—meaning the predator has contacted them on the phone or asked to meet them in person.

B. Pornography

The Internet has also exponentially increased the presence of, and market for, child pornography. Child pornography, most of which is now distributed via the internet, is a multi-billion dollar per year industry worldwide. There are more than 4 million pornographic websites or 12% of all websites. According to data from the National Center for Missing & Exploited Children (NCMEC), located in Washington, D.C., 19% of identified offenders had images of children younger than 3; 39% had images of children younger than 6; and 82% had images of children younger than 12.1 Our law enforcement agencies around the globe are working to combat this crisis.

¹ http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en X1&PageId=1742

In the U.S., an entire section of our Department of Justice is dedicated to "Child Exploitation and Obscenity." The FBI has developed the "Innocent Images National Initiative" which provides a centralized point of communication and information for local, national, and international governments and law enforcement bodies.

Last month, Spanish authorities announced the arrest of 121 Spanish citizens in the largest child pornography bust in that nation's history. The ring was distributing online child porn in 75 nations. Japanese police have taken action in 300 cases of child pornography in 2008 alone. In Australia, the Australian Federal Police Online Child Sex Exploitation Team (OCSET) investigates national and international cases of child exploitation. ISPs in Denmark, Finland, Italy, Norway, and Sweden already block known child pornography sites. And recently in New York, the Attorney General has developed a Code of Conduct for ISPs designed to stop the flow of child pornography. Every major ISP in the U.S. has signed it.

The Council of Europe's Convention on Cybercrime², which requires all signatories to make production and distribution of online child pornography a criminal offense, has been signed by 43 states and ratified by 16. I urge other nations to join this Convention, making our international laws more uniform and hopefully deterring predators around the world.

The U.S., like many other nations, is continuing to update and revise its child protection laws. Earlier this year, the U.S. Supreme Court upheld a law that prohibits

² Council of Europe: Convention on Cybercrime, 41 I.L.M. 282 (March 2002).

the intentional solicitation or offering for sale of child pornography—whether the images are of real or simulated children.³

Likewise, other nations' laws include:

In India, it is a crime punishable by up to 5 years in jail to electronically transmit any material which appeals to the prurient interest.⁴

In France, assisting in the corruption of a minor is punishable by 5 years' imprisonment and a fine of €75,000. The penalty is increased to seven years' imprisonment and a fine of €100,000 where the minor is under fifteen years of age.⁵

Earlier this year Google signed a deal with Brazil's top social networking site Orkut, through which the company will facilitate evidence gathering when there is a suspected case of child exploitation.

The proliferation of child pornography is real and without appropriate government, industry, and community oversight it will likely continue to grow.

Cyberbullying C.

Another threat arising from inappropriate internet use is now a recognized behavioral disorder known as cyberbullying. You may have read the tragic story of a U.S. teenager who took her own life earlier this year after being taunted (by a parent!) online. I-safe reports that 42% of children have been bullied online, and 1 in 4 has had it happen more than once. Psychologists posit that the physical distance between the

7

 ³ U.S. v. Williams, 553 U.S. ____ (2008).
 ⁴ India Information Technology Act of 2000
 ⁵ France Penal Code, Article 227-22

abuser and the victim often make the harassment more aggressive than what would occur in person.⁶ Having been involved in mental health policy for many years, we now recognize that the internet is also facilitating a very real new field of disorders just as concerning as threats to their physical well-being, and often more difficult to prevent given the pervasive and sometimes anonymous nature of internet communications.

D. Child Trafficking

Another concern that has grown with the proliferation of the internet is child trafficking—children being bought and sold online for sex. In the U.S., the Innocence Lost National Initiative has shown that websites like MySpace and Craig's List (commonly used U.S. website for buying selling consumer goods) are being used to advertise victims and services. Traffickers also use websites to recruit their victims. I understand these websites are now requesting more complete information about individuals seeking to post ads. I hope this will have a positive effect. The UK has developed "safemodelling.org.uk", a free advice and information site to protect against scam modeling agencies and rogue photographers. I continue to urge ISPs to be aware of the child trafficking issue, and to cooperate with law enforcement to protect the children in their communities.

III. Global Concern

Law enforcement officials are utilizing and enforcing statutory provisions for criminal behavior. This is post ante—or after an illegal act or harm to a child has

⁶ The New York Times, August 26, 2004.

occurred. Today's discussion is about educating, preventing, and protecting our children's precious lives before injury occurs. Thus, I am here today not only as an American, but also as a global citizen. In just the last few months, I've traveled to speak on this issue at APEC-Tel, the Asian Pacific Telecom Ministers in Bangkok, and at the Global Forum in Italy. I've had the privilege of meeting with ministers from a variety of nations to hear what they are doing to protect children in the online world. While certainly not exhaustive, I have included a few examples of the many international initiatives.

IV. Global Initiatives

Just two weeks ago, the European Parliament voted to set aside 55 million euros to create the EU Safer Internet program, which will promote awareness among children, parents and teachers of how to stay safe online. It will also provide the public with national contact points for reporting illegal content and bring together researchers to establish a knowledge base on the use of new technologies. The EU also funds the newly-established "European NGO Alliance for Child Safety Online" (eNASCO). eNASCO is a coalition of children's rights NGOs from EU Member States working to promote online child safety.

The United Kingdom's Office of Communications (Ofcom) recently recommended to the Mobile Broadband Group, a consortium of the 6 largest U.K. mobile operators, that they strengthen provisions of regulations designed to prevent

minors from accessing adult content online. Ofcom also recommended a voluntary opt-in system that would allow children to access only child-friendly content.

The Ministry of <u>Japan</u> is issuing notices urging parents and schools to limit internet-accessible cell phones to children. They have recommended that Japanese cell phone manufacturers include GPS in every phone, and limit children's phones to talk capabilities only.

In September, the Polish NGO Nobody's Child Foundation and <u>German NGO KlickSafe.de co-hosted a forum called "Keeping Children and Young People Safe Online"</u>. At that conference it was established (through research conducted in Poland and Germany) that children fear being targeted by their peers, more than by internet predators.

NetSafe, a New Zealand organization aiming to provide cyber safety, security, has produced a program called "Hector's World," for New Zealand, Australian, and UK audiences. This program targets children 2-10 with animated characters teaching positive lessons about online safety.

In Brazil, the Senate created a Special Investigation Committee (CPI) to inquire into pedophilia, cybercrime, and any possible links to organized crime. It is expected that out of this inquest may come enhanced legislation and increased law enforcement cooperation (and perhaps a more official role for Safernet, a Brazilian NGO that has an online reporting mechanism for various crimes).

VI. Private Sector Response

In addition to the government and law enforcement initiatives, our private sector partners have been active participants as well—developing voluntary, self-regulatory solutions. That is why today is so important—all sectors uniting to share, to build, to discuss, and to take action. In this age of convergence, it's important to include telecom, wireless, wireline, and media companies. Let me share a few examples from some good corporate citizens—many of the world's top internet and telecom companies and their specific child online protection programs.

AT&T developed the AT&T Hometown Tour, which visited more than 100 communities nationwide and worked with more than 20,000 students from Connecticut to California on Internet safety lessons, programs, and workshops geared toward elementary- and middle-school-aged students. Students participated in fun hands-on activities that focus on key Internet safety skills, such as protecting computers against viruses, hackers and spam, as well as reviewing age-appropriate, good-computing habits, such as proper downloading of legal (non-pirated) material and research-referencing. The program also emphasized keyboard skills, potential dangers associated with social networking, and lessons on stranger-danger.

<u>Verizon</u> announced earlier this year that it will provide free Internet safety tools for parents. This includes a content blocker, application filters, and the ability to set time restrictions during which the Internet cannot be accessed. For cell phones, they have four categories of protection—broken down based on child's age and each

allowing a varying amount and degree of objectionable content— to be set at the parent's discretion.

Sprint has 4NetSafety, which provides children, teachers, parents, guardians and other adults tools and information about online safety. This is a partnership with the U.S. National Center for Missing & Exploited Children and the National Education Association Health Information Network (NEA HIN).

DOCOMO, the largest Japanese wireless provider, has even undertaken an internet-safety curriculum and actually sends instructors into schools to provide instruction. 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.

Microsoft X-box. When first introduced, many parents thought that Microsoft X-Box was nothing more than a game console; yet it houses a system that functions as a highway to the Internet. I am pleased that Microsoft created tools that allow children to play only games with certain ratings, as set by parents. Microsoft's Family Settings also enable parents to prevent children from linking to other players over the Internet for multi-player gaming and let parents limit game play on a daily or weekly basis.

Beyond the Xbox 360 Family Settings, parents can use Microsoft's family safety tools to monitor their child's computer use -- from filtering Web content and managing email contacts to receiving reports that show which sites their child has visited on the Web.

Cox Communications held their third annual National Summit on Internet

Safety—to launch a national dialogue and hear what teens are experiencing first-hand.

This year the Summit, co-hosted by Miss America Lauren Nelson, focused on tweens, children between the ages of eight and twelve, and included parents and caregivers.

Through the Summit it was learned that tweens' online presence doubles or even triples between the ages of eight to ten and eleven to twelve, and one in five tweens have posted personal information online. Communications between parent and child are just as important in the online world as they are in the offline one.

<u>Comcast</u>, the leading residential internet service provide in the U.S., provided – free of charge – a PBS documentary called "Growing Up Online" throughout the month of June, Internet Safety Month. This documentary gives parents a very real glimpse into what teens are doing online. Comcast also has a "For Kids" and "For Parents" resource page online that provide internet safety advice and information.

<u>Charter</u>, another major American ISP and cable operator, provides all of its

Internet customers with the Charter Security Suite free of charge, including two levels
of parental controls – one for younger children and one for teens. Charter has an
ongoing Internet safety education program through the resources available at
www.charter.com/security. This includes an Online Safety Guide for Parents, an
Online Safety Guide for Kids, and links to Amber alerts and the National Center for
Missing and Exploited Children as well as an online form that Internet users can use to
report possible child pornography or exploitation on the Internet.

As with most public policy issues, I believe that government agencies should tread cautiously before exploring heavy-handed regulation. Fortunately, technology may be creating the solutions—but we must provide parents, teachers, caregivers, and even children with a forum to create awareness and share knowledge in a coordinated effort.

V. Solutions

Thus, while our nations may differ regarding philosophy or specific regulatory oversight, we must all work together to develop solutions to the threats our children face online. Today's session is an historic start. Now that the dialogue has begun, I would suggest the following: First, I believe we need an internationally-recognized forum for digital research, online behavioral practices, medical and psychological reports, and experimental studies. Second, we must continue to disseminate this information, to discuss and understand the technology, the threat, and the tools available to protect children around the world. Coordination among nations is vitally important because the internet connects and touches us all-- and all of our children. Third, through this sharing of research and expertise, we need to develop a clearinghouse of best practices, concepts that other nations can replicate. The ITU website which is under development is a first step so that leaders, industry representatives, teachers, and parents can link to successful real-world approaches. Fourth, we need leadership at all levels—from those of you here today representing your respective nations at the highest levels of government, to local municipal and city leaders, as well as media and industry partners, and teachers and caregivers in each of our nations and states.

VI. Conclusion

The Internet and broadband have literally brought the world to our children. With the click of a mouse, or the push of a button on a cell phone, they have access to an endless array of information. Broadband and the internet improve access to healthcare, drive commercial transactions, and allow for instantaneous worldwide communications—literally enhancing every sector of our economies. As technologies converge, the opportunities are endless. Telephone calls, stock quotes, news headlines, photos from Skybar, video games, and internet-- all from the same provider, on the same device. However, as we have seen, these dazzling innovations and life-changing services and products for consumers bring challenges and even risks—risks to our very personal cybersecurity, our privacy, and most importantly, 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. Mr. Secretary, fellow colleagues, it is an honor to be here today and I share the ITU's goal of increasing safety, decreasing fear and expanding the benefits of information and communication technologies, particularly for children around the globe—from Timbuktu to Tennessee and beyond. Thank you.