

Testimony of Teri Schroeder
Chief Executive Officer/Program Director, i-SAFE America, Inc.
Before the House Energy and Commerce Subcommittee
on Oversight and Investigations
United States House of Representatives

April 4, 2006 Washington DC

Thank you, Chairman Whitfield and Ranking Member Stupak for inviting me to testify before the House Subcommittee on Oversight and Investigations at the hearing entitled “Sexual Exploitation of Children over the Internet: What Parents, Kids and Congress Need to Know about Child Predators.”

Predatory acts against our children are among the most heinous of crimes perpetrated within our society. Historically, communities as a collective take deliberate and specific actions to protect their children in an effort to prevent these heinous acts. These protective actions include: education – teaching children to be wary of strangers, to recognize and avoid dangerous situations, to cry for help when they feel threatened.

Our nation is now faced with technological advancements that allow even the youngest of children to have access to the Internet. Students today explore the wonders of the world by transporting themselves through cyberspace. They can travel to the brightest most intellectual domains of the universe and conversely, they may travel to the darkest most detestable realms of the human imagination; and they travel this world alone. A universal paradigm shift has occurred in the methods and means available to child predators in pursuit of their prey; and as such a universal paradigm shift has occurred on the preventative tactics that we employ in our efforts to protect our nation’s youth against these predators.

The content of my testimony today will address the ramifications of this universal shift as our nation’s youth explore the wonders of the Internet. We truly are a global economy and as such our

nation's youth are cyber citizens engaging in online activities. Those activities include socialization (two way communication whether that be through email, chat or instant messaging), games, shopping, entertainment and education.

I will be addressing the role of education and youth empowerment and the need to empower our nations youth with the appropriate tools to minimize the number of predatory acts predicated against them. It is imperative that a proactive well-balanced approach be deployed to support the challenge of embracing the activities of our nation's youth online.

i-SAFE America is dedicated to: 1) implementing a standardized Internet safety education program throughout the nation that provides kids and teens with essential tools to reduce the risk of their being victimized while engaged in activities via the Internet; and 2) launching an Outreach Campaign that empowers students to take control of their online experiences and make educated, informed, and knowledgeable decisions as they actively engage in cyber activities. From September 2005 through March 2006 i-SAFE educated over 1.3 million students nationwide. That number continues to increase monthly as the i-SAFE program is expanded throughout school districts.

The i-SAFE Internet safety curriculum is a teaching and learning experience, which incorporates best practices as they are defined by the latest educational research, and correlates them to accepted educational standards. This is accomplished by providing a broad range of materials and formats which meet a variety of teaching and learning needs for students and educators in grades Kindergarten through 12. Topics are centered on up-to-date information pertinent to safety issues, which confront today's youth through continuing advances in Internet technology.

The curriculum creates a successful learning environment through a model of integrated critical thinking activities and guided opportunities for youth empowerment. Active participation in i-SAFE

student activities promotes acquisition of knowledge, analysis of online behaviors, construction of solutions to Internet safety problems and issues, and involvement in the spread of Internet safety concepts to others through peer to peer. Through this process, students enhance and enrich their own lives, the lives of other students, and the community at large as they engage in creating a safer cyber community.

Our children now live in two diverse worlds: their physical world and the world of cyberspace. As such, they essentially live in two cultures that often conflict. Previously, many of the lessons learned in the physical world don't seem relevant in cyberspace as these children reach out to strangers as friends. This paradigm shift demands new innovative educational programs, and tools, for our children; their parents and the community. It is essential that children, as they travel their world of cyberspace alone, be provided with the knowledge and tools they need to independently recognize and avoid dangerous situations online; to actively engage learned proactive techniques to more safely interact with strangers online; to critically appraise situations in which they find themselves; and to react appropriately when they find themselves in uncomfortable, compromising, or threatening situations.

Students today will be global citizens for the rest of their lives. Students view the Internet in a much different way than adults.

I would now like to address the "Parents Internet Assumptions" and the "Youth Perceptions/Behavior regarding the Internet." At the time of this report approximately 100,000 students had participated in the survey process; students participating in our US program by grade level were:

- 15,000 K – 2 students
- 22,200 grades 3 & 4
- 62,800 grades 5 – 12

The i-SAFE assessment results show that in most cases there is a noticeable difference in a student's participation in risky behavior from grade to grade. Older students are more likely to take risks and/or feel safe in the Cyber world. This finding reinforces the need to introduce and educate our youth in

the early grades. For example: When asked if they had visited an “inappropriate” website; 15.5% of 5th graders said yes vs. 36% for 10th graders.

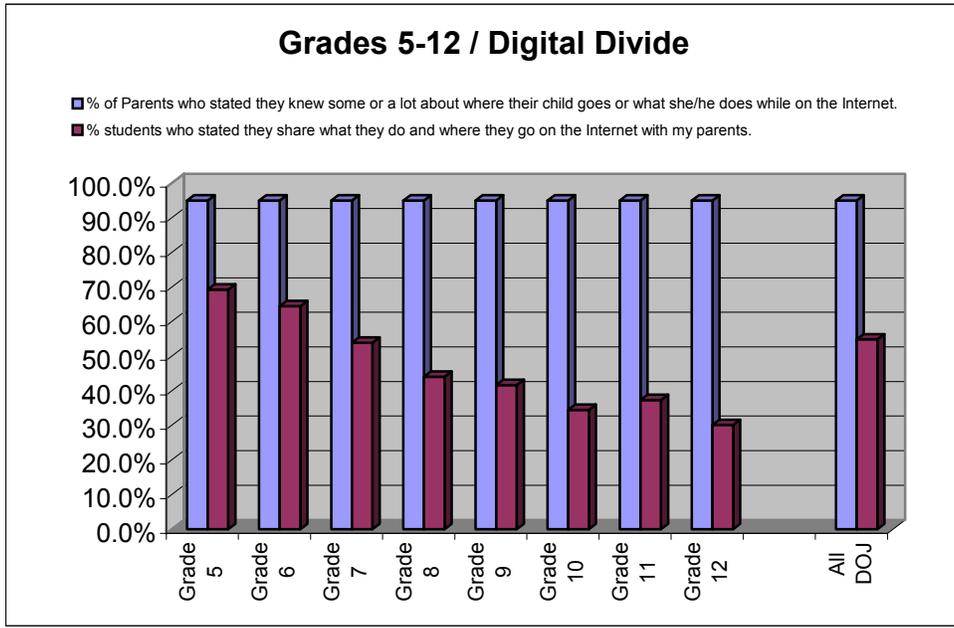
Relative to gender; males are more prone to visit an inappropriate place on the Internet than females (31.3% vs. 18.7%) and are likewise greater risk takers when asked if they were willing to meet someone from the Internet “face to face” (19.2% vs. 11.2%). Males were more likely to play games as their primary online activity while females were more likely to chat or use email.

Also, based on pre assessment results; it is evident that once a youth enters cyberspace there are no significant differences in behavior between ethnic groups. Therefore, the Internet has become the great equalizer. 90.4% of students’ in grades 5-12 and 84% of students’ in grades 3 & 4 have Internet access. And on an average 37% of all 3rd & 4th graders use some form of Internet communication; that figure rises to the 80-90% level in the upper grades. Interestingly, about 45% of students in grades 8-10 stated that online communications were their main method in keeping in contact with friends. In addition students in grades 5 –12 stated that:

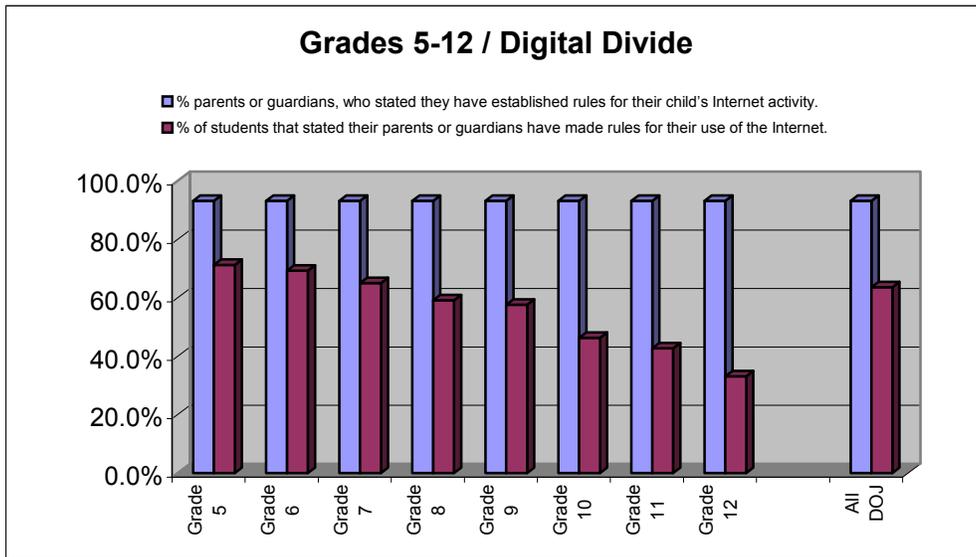
- 23% are online for more than 5 hours a week (86% are online at least 3 hour a week).
- 8% have been asked to keep their Internet friendship a secret.
- 12% have been upset by something that was said by a stranger they met on the Internet.
- 32% have the skills needed to get past filtering software and 20% have actually used those skills to get past filtering software.

Digital Divide Between Parents & Youth

There is a gap between what parents say they know and what youth claim they share with their parents. In an i-SAFE survey with over 2,000 parents, the vast majority (94%) of parents stated they had a pretty good idea about their child’s online behavior. In contrast, only 54% of the students said they share where they go and what they do on the Internet with parents. Our results also show that these differences between parents and students generally increase with increasing age.



Of the parents surveyed, 93% felt that they had set ground rules for their child’s online activities. However, the percentage of students acknowledging that their parents had established rules for their Internet use drops to 63.7% (see chart below).

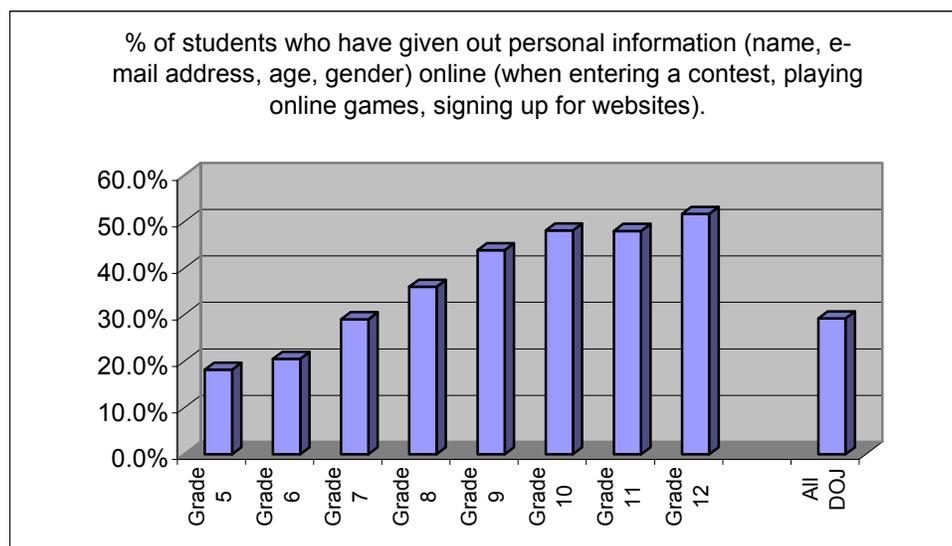


In addition, 21% of the students stated that their parents complained about the amount of time they spent on the Internet but 29% also felt that their parents really had no idea how much time they were actually spending online. 62% of the parents polled indicated that they were NOT concerned about the

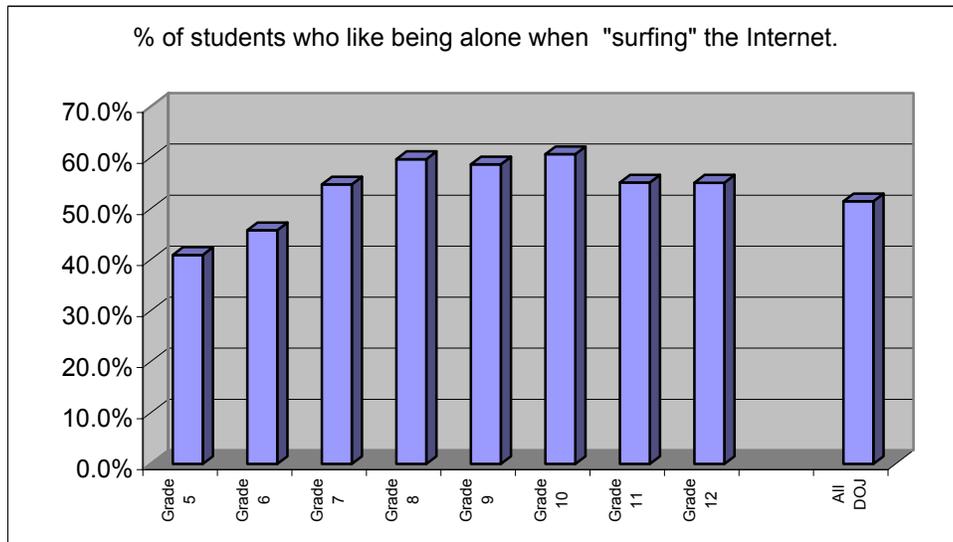
amount of time their child spends online. Interestingly, on average, 25% of the students stated that their parents, on some level, would disapprove of their online activities and 13.8% actually keep their Internet activities secret from their friends and family. The gap between what youth believes to be their parent’s level of awareness regarding their online behavior and what parents have stated is significant and merits continued attention.

At Risk Behaviors

There are other individual statistics that underscore the need for constant Internet safety education. For example, the Internet has become a focus for youth to find entertainment, make new friends and make purchases. On an average 29% of the students have shared such information when going online. That figure goes up in the 50% in the higher grades.



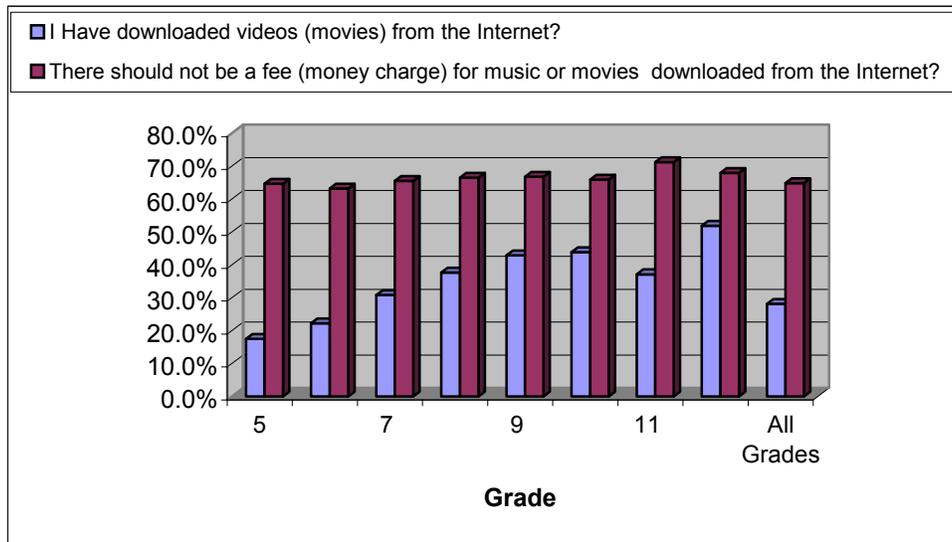
Two other factors compound this issue. More than half of all students prefer to be alone when accessing the Internet (see graph below). Combine that desire with a student having their own computer in their room (22% overall stated that the computer they use is in their bedroom); and students feel empowered or freer to do what they want on the Internet than they do in the real world (33%).



It should be pointed out that even in the very early grades our youth are being exposed to the cyber world. It is folly to suggest, as some have stated, that “kids that are young are not Internet savvy.”

The vast majority of K-2 teachers (54%) stated that at least 50% of their students have used a computer at home and 16% of the teachers indicated that at least 50% of their students have used email. A significant number had also gone into chat rooms. The age demographics of these students consist of 5, 6, & 7 years olds.

28% of all students in grades 5-12 (43-52% in the upper grades) have downloaded music or movies from the Internet. On an average, 65% were against any type of fee being charged for the service.



In real life Kids/Teens spend twice as much time with peers as with parents or other adults. However, through the guise of anonymity the Internet provides a medium which allows a student to believe that the communication they are having online is a respective peer when in many instances it is an adult. Even though students may be aware of the dangers inherent in communicating with someone online, we continue to see they make decisions about engaging in a behavior as if it were a one-time thing.

Risk taking is a natural part of kids/teens lives. They take risks in order to grow, trying new activities, generating new ideas, experimenting with new roles. However, they can also find themselves in trouble with their risk taking. Concern over such risk behaviors have led to the creation of many types of intervention. Some of these interventions have attempted to manipulate kids/teens beliefs, values and behaviors hoping to get them to act more cautiously. Other interventions have attempted to improve their stability to make sensible decisions, hoping to get them to make wise choices on their own. Having general decision-making skills enable kids/teens to protect themselves in many situations.

Education Makes A Difference

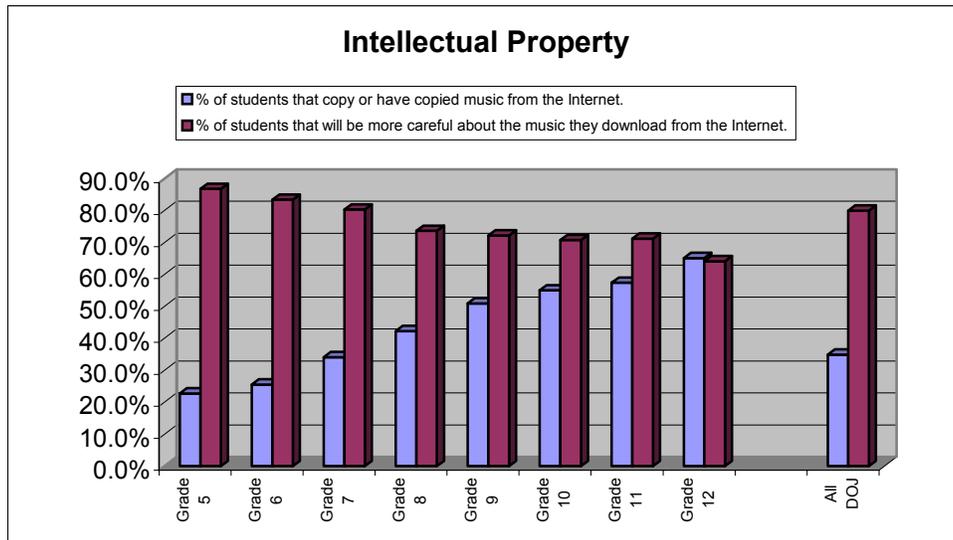
The good news is that in-classroom education and outreach efforts do make a difference. Students taking i-SAFE post assessments, immediately after completion of the i-SAFE curriculum, demonstrated a significant rise in their Internet dispositions.

84% of students stated an intention to be more careful about where they go and what they do on the Internet.

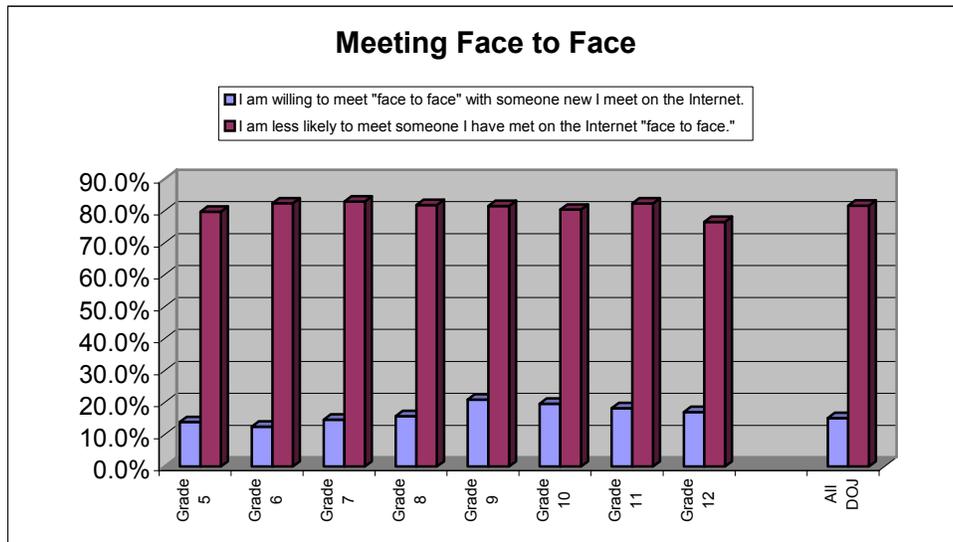
89% indicated that they would be more careful about the email attachments that they open.

88% will be more careful about sharing personal information with those they meet in chat rooms and other places on the Internet.

On an average, 80% of the students polled after completing the i-SAFE program were going to be more careful about downloading music from the Internet. However, older students were more inclined to download and less concerned about being careful.



An area that attracts quite a bit of attention is child predation. Our pre assessment data shows that on an average about 15% of the youth were willing to meet someone new from the Internet “face to face”. After the i-SAFE program 82% of all students stated that they would be less likely to meet someone face to face.



Though individual statistics can be interesting and in some cases alarming, the real power of the data lies in the overall trends that reveal the impact of emerging cultural and social changes brought about by the Internet. The increasing amount of time spent in the Cyber world, the ability to remain “anonymous”, the perceived lack of rules, the ease of access; all contribute to a revolution in the way our youth interact with each another, the way they make friends, and the social skills they develop.

It is widely recognized and accepted that the main activity of kids/teens, as cyber citizens, is online two-way communication. That communication consists of chat, email and instant messaging. The nucleus of the Internet affords the opportunity of two-way communications and inherently the computer does not know whether the users communicating are that of a child or an adult. This means of communication allows users, regardless of age, gender or socioeconomic status to openly and freely exchange ideas and information. Our nation’s youth has now coined a new term for “ hanging out with my friends” and actively searching for new friends is done through a click of a mouse.

Kids/teens rarely “travel” with their parents or a chaperone to many of the online areas. Buddy lists and instant messaging has replaced the traditional “telephone and phone book.” Without education and the appropriate tools to raise their awareness and to empower them to recognize the danger of being alone in a room full of strangers, our nations youth will continue to be at risk for exploitation.

Let me begin by addressing specific examples of how dramatically the protective actions that have been employed historically have been impacted by this technologically-enabled, Internet-driven, paradigm shift.

Education: Parents teach children to be wary of strangers on the street, in public places, and at the front door; but now, the strangers that these children meet – are not on the street – they are in cyberspace. And, to the detriment of the parents, many of their children are more “Net” savvy than either parent. This inequality of knowledge hinders parents in their abilities to address cyber safety issues and to properly instruct their children about the dangers of meeting strangers online.

Historically, when parents taught their children to recognize and avoid dangerous situations, those situations were based on tangible, physical elements within their community. Now, danger lies in an amorphous cyber-world cloaked in the allusion of anonymity.

Parental Supervision: Many of our children’s activities have dramatically shifted from participatory activities (easily supervised by a parent and often enjoyable to watch) to solitary activities - engaged through the computer keyboard or joystick - that do not lend themselves to easy supervision nor enjoyment by a non-participant (such as a parent). Children may spend hours playing solitary games online, or they may play in tandem with their cyber friends, or they may even play with total strangers they connect with online in an Internet gaming community.

The Internet has broadened a child’s ability to meet other people and acquire “friends.” Historically, children made friends at school, through family acquaintances, and from participating in community organizations. A child is no longer confined to the local community from which to socialize and gain friends; literally, cyberspace eliminates all geographical barriers and frees a child to roam the world in search of that one, special “friend.” Predators are also free to roam.

The degree of difficulty for parents to monitor, or to simply meet, their child's friends has increased tremendously.

Preventative Tactics: A commonly employed tactic for protecting our children is to provide an adult chaperone as our children explore outside of their community. Now, children explore the wonders of the world by transporting themselves through cyberspace and they travel this world alone, without the care and protection of a chaperone.

Physical Barriers. Historically, parents routinely lock their doors at home each night to keep intruders out; schools monitor persons who enter the campus. There are innumerable, vulnerable children who are isolated, lonely, and bored who constantly search the Internet for other children with whom they can make friends and chat. As these children search the web for friends so too the predator searches the web for prey. The predator will find the child, the child will find a "friend," and the outcome will be devastating.

The effectiveness of currently employed physical barriers has been severely compromised. Predators lure and seduce their victims from within the privacy of the victim's own home and operate in a world that is no longer constrained by physical limitations or geographical barriers. They stalk their prey through cyberspace and the ramifications of this universal, paradigm shift are staggering. When taken as a whole they can be overwhelming, perhaps paralyzing; but - if ignored - the ramifications will be devastating to our youth. To approach any entity of this magnitude and to effect change it is advisable to search for a common element, theme; or component against which a focused solution may be enjoined.

Up to this point in my testimony, I have provided insight into the incredible paradigm shift that has occurred in our society and how this new paradigm directly affects the safety of our children. To

illustrate the critical points, I mapped the ramifications of this paradigm shift to a common element in cyberspace: two-way communication (ie. chat room, instant messaging and email)

The remainder of my testimony will focus on potential solutions that we as a society may embrace as our children extend into the farthest reach of cyberspace; as they interact virtually with persons throughout the world and as they evolve as “Net” citizens.

As Judith F. Krug, Director of the American Library Association’s Office for Intellectual Freedom, stated in her testimony before the COPPA Commission on August 3, 2000: “The children of today will be Net citizens for the rest of their lives. They need to be taught the skills to cope in the virtual world just as they are taught skills to cope in the physical world. Children should be educated in appropriate increments and appropriate settings on how to avoid inappropriate Internet content, to report illegal or unsafe behavior and to engage in safe interaction online. Children who are not taught these skills are not only in danger as children in a virtual world, they also will grow into young adults, college students and an American workforce who are not capable of avoiding online fraud, Internet addictions and online stalking.”

It is imperative that any domain that engages in the attraction of kids/teens recognize how children actually use the Internet. It is equally important to promote the online social activities within the domain to support the academic strategies that teach children to make safe and wise choices about using the Internet and to take control of their online experiences: where they go, what they see, to whom they talk, and what they do.

Our nations youth need to be given the tools to assist them in the acquisition of skills that will allow them to evaluate independently the information they are acquiring and exchanging online. By improving their "information and media literacy," they will become safe and responsible cyber citizens

thus vitiating the “digital divide” that exists today between Youths Perception/Behavior regarding the Internet and those of their Parents.

Currently, both businesses and governmental agencies have begun to embrace digital certificate technology as an electronic means for identifying participants in transactions that occur online. They leverage this technology as a method for verifying and authenticating a person’s electronic identity. The simplest way to view a digital certificate is as an electronic ID card. However, digital certificate technology is far from simple. Given that the intent of this testimony is to identify and express how technology can be used, rather than to define the intricacies of the technology, I will refer to digital certificate technology in the simplest terms possible for the reader to understand.

A certification authority issues digital certificates. A certification authority can issue various levels of digital certificates that are dependent upon the amount of authentication that is required to ensure that the person who is applying for the digital certificate is in fact the person that he or she claims to be. In other words, to obtain a digital certificate a person must present proof of identity and the “level” of the certificate obtained depends upon the amount of proof required.

- Example:
- Level 1 certificate - any photo ID required
 - Level 2 certificate - government issued photo ID required
 - Level 3 certificate - government issued photo ID required plus passport or birth certificate
 - Level 4 certificate - all requirements of Level 3 plus a background check
 - Level 5 certificate - DNA

How could digital certificate technology increase the safety of children who frequent a particular chat room or deploy two-way communications on the World Wide Web?

A public- or private-sector chat room provider could engage digital certificate technology as a means for permitting or denying access to any given chat room or online area that allows two way communication. Conceivably, a chat room provider could institute a policy that only children under the age of 13 are allowed to participate in a particular chat room. The intent of this policy is to provide a safer online environment by making their “best effort” at excluding adults and potential pedophiles from the chat room. To enforce the “under the age of 13” policy, the chat provider would require all participants to login using a Level 3 digital certificate. Through the use of the digital certificate and the chat provider’s policy of restricting access, the children participating in this chat room have a lessened degree of risk than those children that participate in unrestricted chat rooms.

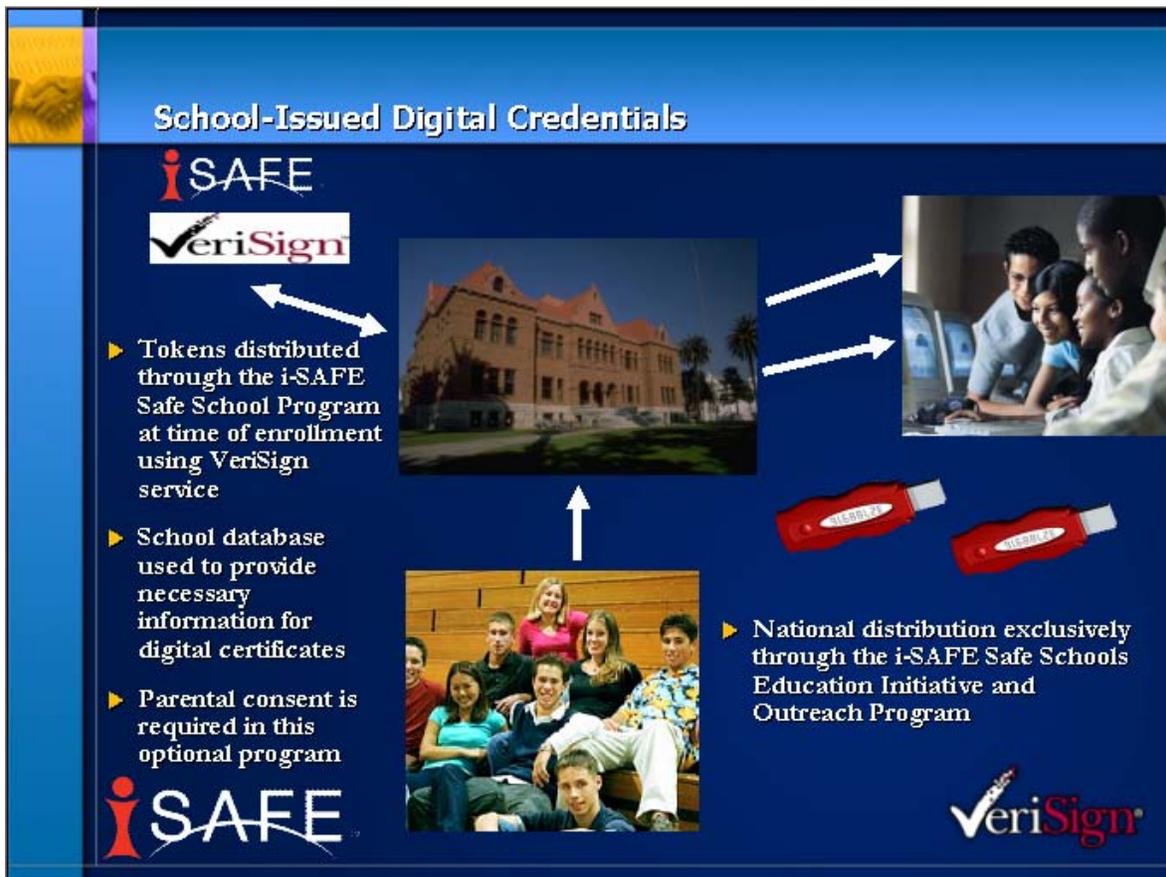
This technology exists and i-SAFE, through the empowerment of our partnership with Verisign, has launched the first tool for our nation’s youth, using digital certification. The unprecedented Digital Credential program, “i-STIK” works to reduce the vulnerability of America’s students in all grades, K-12, with a unique digital credential that helps protect students as they engage in two way communications online.

The Digital Credential is in the form of a small USB Token, which can be carried on a key chain and used at school, home; or on any computer with a USB port. The Digital Credential allows the kids and teens to enter an age centered chat room, or conduct two way communication, with confidence that everyone logged in will be who they say they are – chatters actual ages and genders can be confirmed from the digital credential token. The digital credential helps to safeguard the integrity of the child’s online experience.

The digital credential is distributed through the i-SAFE Safe School Program at the time of enrollment (with parental consent) helping confirm to parents that this program is offered through a trustworthy source.

The schools database, which remains with the school, provides all the necessary information contained on the digital credential and validation is provided to assure that the token is valid at the time of usage. Neither i-SAFE or Verisign has access to this information. The identity of the student is never disclosed, just the students age and gender. The program allows for easy revocation of the credential when the student transfers, graduates or is not longer enrolled in the schools.

I am showing you screen shots of how this new tool will be deployed and the interaction between the user and technology.



We currently use digital certificates to execute online financial transactions. Businesses use this technology to protect their monetary assets. In September of 2005 there was a deployment of a pilot project that allowed parents to opt in to have their son/daughter be issued their first digital certificated which is being deployed nationwide as the “ i-STIK.”.



Usage of Tokens

- ▶ **Tokens are portable containers for a child's digital credential**
 - Use on any USB port
 - Can be carried around on a key chain
 - Can be used at school, at home, or in any computer with a USB port
- ▶ **Digital Credentials only contains necessary info for usage online**
 - Gender
 - Age

iSAFE **VeriSign**

Protecting our children is at the very heart of this hearing. Thank you Chairman Whitfield and Ranking Member Stupak for inviting me to testify before the Subcommittee on Oversight and Investigations. In my testimony, today, I addressed the paradigm shift that has occurred within our society due the advancements in web technologies and the advent of two way communications that could be deployed to facilitate the establishment of an enjoyable environment for our nations youth. I have touched upon one technological approach that i-SAFE is launching to empower our nations youth with a “tool” to help protect our children from falling victim to online predators.

In conclusion, there is no single solution for protecting our children. However, the value of empowering our children - through “**education**” – with the knowledge and critical-thinking skills that they need to be able to independently assess the every-day situations they will encounter, while online, cannot be overstressed. Children must be able to effectively protect themselves from cyber predators, to recognize potentially harmful or inappropriate actions, to actively disengage from negative behaviors or compromising situations, and to seek help when threatened. These lessons are learned. Education and empowerment are key.

The First Digital Credential Program for America's youth.



➤ The Facts

A 2003 iSAFE America study shows that nearly 11% of kids and teens have met someone "face to face" who they "met" online.

Considering that more than 50 million youth in the United States use the Internet and countless online predators lurk in cyberspace waiting for unsuspecting victims, **millions** of American kids and teens are **at risk** of abduction or worse.

A lack of valid age authentication in the online areas kids and teens surf the most has compromised the safety of those who use those chat rooms, Instant Messaging services, and other public online areas.

Some websites allow the purchase of alcohol, cigarettes, and adult materials with the only validation being a credit card – no age verification is required!

➤ The Solution

On February 10, 2004, a revolutionary new way to help protect the safety of America's kids and teens online is officially introduced.

iSAFE America, the nation's leader in Internet Safety Education and VeriSign, a leading provider of critical infrastructure services for the Internet and telecommunications networks, have partnered to create a groundbreaking program that provides the most innovative degree of online safety previously unavailable to our nation's youth.

The **unprecedented** Digital Credential Program works to **reduce the vulnerability** of American students in all grades (K-12) with a unique digital credential that helps protect students as they surf the Internet.

➤ The Empowerment



➤ The Technology

The Digital Credential is in the form of a small USB token, which can be carried on a key chain and used at school, home, or any computer with a USB port. Besides the convenience of portability, the Digital Credential provides a foundation for additional features such as a personal data storage device.

The Digital Credential allows kids and teens to enter an age-centered chat room with confidence that everyone logged in will be who they say they are – chatters' actual ages and genders can be confirmed from the Digital Credential token. The Digital Credential helps to safeguard the integrity of the child's online experience.

The Digital Credential is distributed through the iSAFE Safe School Program at the time of enrollment (with parental consent), helping confirm to parents that this program is offered through a trustworthy source.

The school's database provides all the necessary information contained on the digital certificates and VeriSign provides validation to assure that the token is valid at the time of usage. The identity of the student is never disclosed, just the student's age and gender. The program also allows for easy revocation of the credential when students transfer, graduate, or are no longer enrolled in the school.

➤ The Future



iSAFE has partnered with the American Football Coaches Association on their National Child ID Program. The paw imprint of iSAFE's cyber dog, Browzer, is indicated within the token if a student has been ID'd through the iSAFE/AFCA alliance.

The Digital Credential helps to build a natural association of online safety through its branding.

VeriSign will manage and update the service integrity of a national database which contains every participant's information.

References:

NTIA and Economics and Statistics Administration. A Nation Online: "How Americans Are Expanding Their Use of the Internet" published by the National Telecommunications and Information Administration, U.S. Department of Commerce, Economics, and Statistics Administration (02/02)

www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htm

i-SAFE America student assessment data, 2005