TESTIMONY OF

PARRY AFTAB, ESQ.

**(THE KIDS INTERNET LAWYER and
FOUNDER and EXECUTIVE DIRECTOR, WIREDSAFETY.ORG, THE WORLD'S LARGEST AND OLDEST INTERNET SAFETY and HELP ORGANIZATION and TEENANGELS.ORG, ITS TEEN EXPERT AND TRAIN-THE-TRAINERS PROGRAM)**

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON COMMERCE, SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

**APRIL 4, 2006, 10:00 A.M.
RAYBURN HOUSE OFFICE BUILDING, ROOM 2123**

Parry Aftab, Esq.
Executive Director, WiredSafety.org
Email:parry@aftab.com
www.aftab.com

TABLE OF CONTENTS

SUMMARY 3

OPENING STATEMENT 3

SNAPSHOT OF U.S. MINORS ONLINE AND HOW PREDATORS REACH THEM 4

Putting Their Heads into the Lion's Mouth 4

The Anatomy of a Cyberpredator: 6

It Doesn't Take Torture for Them to Spill Their Guts 7

The Script—How They Operate Online 8

Why It Works 8

Anatomy of a Real and Early Case 9

Getting in Under Your Radar: 10

Using Celebrity's Names 11

APPENDIXES: 14

Appendix 1: WiredSafety's Guide to MySpace.com 14

Appendix 2: Parry Aftab Bio and CV 21

Appendix 3: From Parry's Upcoming Book, Internet Safety 1-2-3: 25

Appendix 4: Parenting Online - WiredSafety.org's booklet for parents - printable online 31

Appendix 5: More about WiredSafety.org 39

SUMMARY

Our children are online. They do their homework, entertain themselves, communicate with each other and us, research things, buy and compare prices online. They need the Internet for their education, their careers and for their future. Of all the risks our children face online, only one is certain. If we deny our children access to these technologies, we have guarantees that they are hurt. All other risks are avoidable through a combination of awareness, supervision and parental control and other technologies. More and more children being lured and stalked by online predators who gather information about them from chatrooms, instant messaging, e-mails, websites and the like and use this information to become close to them.

With our children walking around with Internet access in their backpacks and pocketbooks, we can no longer rely on parents watching whatever they do from a central location computer. Our children need to learn to use the "filter between their ears" and "ThinkB4TheyClick." This requires that we get them involved in framing solutions and educating each other. It also requires that we find new ways of building good cyber-citizenship and helping the kids and parents spot risks in new technologies and protect themselves online.

But we also need to recognize that in most cases our children are putting themselves in harm's way. They are intentionally sharing risky information online in profiles, blogs and on websites. They post their cell numbers on their public away messages when using IM technologies. And even when they are careful about protecting their own privacy, their close friends may expose personal information about them by posting photos and information on their profiles. They are also, in greater and greater numbers meeting people offline that they met online. Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47- year old child molester instead. This has to stop.

Smart kids are sharing sexual images online with people they don't know, or e-mailing them to others they have a crush on and hope to entice. And with the newer video-chats and technologies, the predators have moved to luring our kids into posing and engaging in sexually explicit activities.

Yet, the actual statistics are lacking. Everything we know is largely anecdotal. In 1999, the FBI's Innocent Images (charged with investigating crimes against children online) opened 1500 new cases of suspects who were attempting to lure a child into an offline meeting for the purposes of sex. Based upon my estimates, about the same number of cases were opened by state and local law enforcement agencies that year. The same year, approximately 25 million minors used the Internet in the U.S., Now, with more than 75 million young Internet users in the U.S. we don't know if the number of instances have increased, decreased or remain flat, given the growth. The crime reporting forms don't collect information about the use of the Internet is child sexual exploitation crimes, or any other crimes. That has to change.

We also need to recognize the real risks and what is hype. Notwithstanding media reports to the contrary, to my knowledge, law enforcement is not aware of anyone who is using the information children provide online to seek them out offline, by hiding behind a bush or grabbing them on their way home from school. They currently agree to meetings (even if they don't admit it to the police when things go wrong.) But it’s only a matter of time before this happens, since universal access to the Internet means that even violent sexual offenders who are online can use it for their own horrible purposes.

OPENING STATEMENT

Thank you for inviting me to testify here today about ways we can keep our young people safer online. This is a very important topic and one to which I have devoted my life over the last ten years. My name is Parry Aftab. I am an Internet privacy and security lawyer and run the world's largest Internet safety and help group, WiredSafety.org.

We are an all-volunteer group and a charity formed in the United States. We have approximately 11,000 volunteer from 76 countries around the world, all devoted to helping create a safer interactive technology experience for users of all ages.

SNAPSHOT OF U.S. MINORS ONLINE AND HOW PREDATORS REACH THEM

It is estimated that approximately 75 million minors in the Unites States access the Internet either from home, schools, community centers and libraries or from some newer Internet-capable device. This is up more than ten-fold since 1996, when only 6 million U.S. minors were online. Now our children are using cell phones with Internet and text-capability, interactive gaming devices (such as X-Box Live and Sony Playstation Network) with voice over Internet and live chat features, handheld devices with Bluetooth and other remote-communication technology (such as PSP gaming devices and mobile phones) and social networking profiles (such as MySpace, Facebook, Bebo, YFly and others) where they can advertise their favorite things, where they live and pictures of themselves and their friends to anyone who wants to see them.

Ten years ago, when I first wrote my safety tips telling parents to put the computer in a central location, that made sense. It was a central point, where parents could get involved and supervise their children's interactive communications and surfing activities. Now, where they take their communication technologies with them in their pockets, backpacks, and purses, it is not longer as relevant as it once was. Now, instead of expecting parents to watch everything their children are doing online from the comfort of their familyrooms, or kitchen counter, we have to do more. Now, we have to teach our children to use the "filter between their ears" and exercise good judgment and care when using any interactive device. While teaching parents how to supervise their children online was a challenge (I have written the leading books, worldwide, for parents on Internet safety), teaching children to "ThinkB4uClick" is much harder.

When I was growing up (in the days before electricity and indoor plumbing, when we had to walk up hill, both ways!, in blizzards to get to school), parents used to blame us for not behaving. We were disciplinary problems. Now pediatric neuro-psychologists tell us that preteens and young teens are hardwired, through immature brain development, to be unable to control their impulses at this age. Either way, we recognize that preteens and teens take risks, don't appreciate the consequences of their actions and act before they think. When their audience was their school friends, family and neighbors, the risks were containable. When they act out where 700 million Internet users can see, it takes on a much deeper significance.

Putting Their Heads into the Lion's Mouth

Now, I will share something very controversial. While educators and child psychologists understand this, most parents will be shocked at the suggestion that their preteens and teens are in control of their safety online and putting themselves at risk, often intentionally. But unless we accept this, and direct our attentions at solutions aimed at this reality, we are all wasting our time. We will focus on the much smaller segments of preteens and teens who are being victimized through not fault of their own - those who are targeted at random. All others need to change their online behaviors. And that's where we need to devote all our attentions.

For this to happen, you need to understand the truth. For years we have told parents and minors not to share too much personal information online. "You can be tracked down in real life," we told them. But, notwithstanding anything to the contrary reported in the media and by some local law enforcement officers, to my knowledge, to this date, no preteen or teen has been sexually-exploited by someone who tracked them down from information they posted online. In each and every case, to my knowledge, to teens and preteens have gone willingly to meet their molester. They may have thought they were meeting someone other than the 46 year old who is posing as a teen, but they knew they didn't know this person in real life. They are willingly agreeing to meet strangers offline.

What does this mean? It means we can do something about this. It means we can educate teens and preteens about the realities of meeting people in real life they only know in cyberspace. It means we can create solutions. It means that this is, at least for the time being, 100% preventable. It means that what we do today will have an immediate

impact on the safety of our youth. It means we have to join together and work on things that are effective and abandon those that are not.

But we have to act quickly. When I testified before the U.S. House Of Representatives, Committee On Commerce, Subcommittee On Telecommunications, Trade, And Consumer Protection on October 11, 2000, I cautioned:

> Law enforcement is not aware of anyone who is using the information children provide online to seek them out offline, by hiding behind a bush or grabbing them on their way home from school. But it's only a matter of time before this happens, since universal access to the Internet means that even violent sexual offenders who are online can use it for their own horrible purposes. (See Testimony of Parry Aftab, Esq. U.S. House Of Representatives, Committee On Commerce, Subcommittee On Telecommunications, Trade, And Consumer Protection on October 11, 2000.)

Luckily, while our young people are sharing much more information online than ever before, to my knowledge, predators aren't using it to hunt down our children offline. They are like vampires. They need to be invited in. Sadly, our teens and preteens are too often doing just that. They are inviting them to offline meetings, phone calls and videochats. But, as an expert in cyberrisk management, I can tell you that this is good news. Because we have a single point of risk - our children, preteens and teens. If we stop their risky and unsafe behaviors, and teach them when to reach out for help, we can manage this risk. We can keep our children safe.

Our children are mainly at risk because of their own actions. Some are intentional. Others are inadvertent. They may willingly engage in communications with people they don't know in real life "RL," agree to meet them offline or send them sexually-provocative images or perform sex acts on webcams they share with people they encounter online. They cyberbully each other by advertising their victims for sexual services, posting real or manufactured sexually explicit images of them online or by passing online rumors able their sexual preferences or activities.

Preteens and Teens at Risk: Most of the high risk preteens and teens fall into three categories: those who are naive and looking for love and affection (typically the "loners" and "shy" preteens and teens), those who already engage in other high risks activities, such as drug and alcohol abuse, driving too fast or doing risky things for the thrill of it (often the student leaders, athletes, cheerleaders and very competitive teens, the risks takers and thrill seekers looking to let off steam or impress their peers) and those who don't realize that what they do online is real, the ones who are looking to appear older, cooler, more fun and more popular (most of the teens and especially preteens fall into this category at least once). Sadly, most of our preteens and teens fit one of these categories. Sadder still is the fact that in recent years we have learned that most preteens and teens are potential victims.

Naive, loners and socially-shy preteens and teens: Some believe that they are communicating with a cute 14 year old boy, who they later discover isn't cute, isn't fourteen and isn't a boy. Most of the reported cases fall into this category, and until the death of Christina Long four years ago this May, experts all believed that *all* victims fell into this category. They are conned, and easy to spot online. Predators can seek them out, and find their vulnerabilities. They are groomed with care, and often fall in love with their molesters. Sadly, when the molestation finally occurs, not only are their bodies broken, their hearts and trust are too.

They need to understand how the predators work online. Too often they tell me that they can "tell" how old someone is online. They can't. No one can. Many predators spend years cultivating the right tone and language to look like a fellow teen online.

These preteens and teens are sitting ducks. While they may have learned not to fall for the "help me find my puppy" ploy offline, they need to learn how that same ploy (appeal for assistance) works online. They need to know how to spot the risks and the predators, when online everyone can look like a cute 14 year old boy. They need to learn that romance shouldn't occur only in cyberspace, and that parents can get involved to help them meet their soul-mate, assuming they really are. So, if they aren't, and turn out to be a 46 year old child molester, they can come home safely and help put that molester behind bars where they deserve.

Risk-takers, Thrill-seeking preteens and teens: Some preteens and teens (mainly teens) are looking for the thrills and challenge of engaging in a relationship (or at least prolonged communication) with an adult. They "play games" with the adult, and are intentionally extra sexually-provocative. They think they are smart enough to do this without

getting hurt. They see this as a game, without realizing the consequences of their actions. And crossing the sexual line isn't as frightening online as it would be in real life. The problem is that the consequences are not as apparent, the realities not as immediate. They take risks. And they think they can handle them. (They don't often understand the consequences, though.) They often willingly engage in sexual communications with men they know are adults. That's part of the thrill. They are also often willing to engage in sexual activities with the adult, but don't realize what that can mean when things go very wrong. We rarely hear about these kinds of victims, because they never report it when things go wrong. They feel as though they "asked for it," or are to blame. When we hear of these cases, it's because they are killed or kidnapped. (Christina Long was in this category. She was the first confirmed murder victim of an Internet sexual predator in the U.S. and died four years ago this May.)

Friends are the answer here. If we can get friends too help watch out for each other, it is less likely that they will meet adults in real life, or if they do, got alone. Also, finding cool spokespeople, like Nick Lachey, to explain that it isn't cool to be stupid and campaigns such as our "Don't Be Stupid" help. So do real life stories from victims themselves about how they got caught and advice from the trenches. Kateisplace.org has sections specifically directed at this type of victim. And Teen People is an important partner of ours in spreading the word.

Not really a drunken slut, just playing one online: We've all been reading about this new trend in the news (often with me as the expert). Good, respectful, otherwise well-mannered preteens and teens acting out in cyberspace. In profiles, blogs, on social networking sites and their away messages on IM, on their websites and interactive gaming bios, they act out. They pose in their bras, or worse. They simulate sexual activities (and in some cases post images of actual sexual activities). They pretend to be someone or something other than what they really are. And this alter-ego may be a sexually promiscuous teen "up for anything."

They don't think it is cool to tell others they were home coloring with their five year old niece last weekend. Instead they claim to have snuck out after everyone was asleep to get drunk at a wild party. To them it isn't real. They lie. They pose. They do thing online they would never dream of doing in RL. They aren't really drunken sluts - they are just playing one online. (Shannon, one of our award-winning Teenangels, will share insight into why teens and preteens are doing this, during her testimony today.)

The Anatomy of a Cyberpredator:

There have been many cases recently where pedophiles and other adults have lured children into offline meetings and molested them. Luckily, there are even more cases when such attempts to lure a child have brought about the attention of law-enforcement groups. I debated whether I should discuss any of these cases, because I did not want to sensationalize them. But if explaining the methods used by offenders might make parents more aware, and their children safer, it’s worth it.

Cyberpredators, just like their offline counterparts, usually aren’t the scary, hairy monsters in trench coats we imagine standing on a dark street corner. Many are the kind of person you would be inviting to your home as a guest, and often have. They are pediatricians, teachers, lawyers, clergy, vice cops, welfare workers, journalists, Boy Scout leaders, baseball coaches, scientists, etc. They are almost always men. (Sometimes women are accomplices, but rarely are women the molesters.) They are often articulate and well-educated. They come in all shapes, sizes, and colors, and they can be very rich or out of work. But they have one thing in common: they want your child.

Most of us are sickened at the thought of an adult having sexual relations with a child, but to be able to protect our children, we must get into the mind of the predator. First of all, predators often don’t see themselves as predators. They see themselves as loving partners with the children they molest. To them this isn’t rape, it’s a seduction. And, as with any seduction, it’s a slow and painstaking process. (Predators have been known to wait more than two years, collecting data on a particular child, before striking.) That’s what makes them hard to detect. They don’t appear to your child to be dangerous.

An FBI agent who shared a panel with me recently said it best: “Before the Internet, these people had to get physically close to your children. They had to lurk near schoolyards, or playgrounds. Kids would see them. Adults would see them. It was a dangerous situation to be in for them, because everyone would notice an adult male lurking around children. They often had to take jobs and volunteer positions that allowed them to work with children in a

position of trust in order to reach their victims. Now, however, the personal risks the pedophiles had to expose themselves to in order to be around children are gone. Now they can be 'one of the kids' and hang out with your kids online without exposing themselves. As long as they don't say or do something in the public room that makes them stand out, they can stay there forever, taking notes."

And, many of them do. They have been known to create large databases on children. They track the children's likes and dislikes. They track information such as whose parents are divorced, who doesn't like their father's new girlfriend or their mother's boyfriend, or who likes computer games or a particular rock group. Kids often share personal information about their lives in chatrooms or on profiles. This is one reason why they shouldn't. The more the predator knows about your child, the more easily they can "groom" them or appear to be their soulmate.

Some cyberpredators (known as "travelers" to law enforcement) seek out the good kids, the smart ones, the ones who are not street-smart and are from sheltered suburban or rural families. Many of our children match that profile perfectly. Others, however, target (or are targeted by) popular, super achiever, risk preferring teens. It took the death of a young teen from Connecticut, Christina Long, before we realized that many of the incidents involved teens who did not fit the loner profile. What we learned was that these kids never report any attacks or exploitation. The only time we hear of these cases is when the teen is kidnapped or killed.

So who is a typical victim of an Internet sexual predator? Anyone between 11-1/2 and 15. All are vulnerable.

It Doesn't Take Torture for Them to Spill Their Guts

Here's a mock chatroom discussion that my law-enforcement friends and I agree is pretty realistic. Imagine a predatorial pedophile sitting and taking notes on this child, and using this information to lure them later. Would your child fall for this? Most, unfortunately, would. This one is more typical of a boy victim and predator communication than a girl victim communication.

> Child: I hate my mom! I know it's her fault that my parents are getting divorced.
> Predator: I know. My parents are getting divorced, too.
> Child: We never have any money anymore, either. Every time I need something, she says the same thing: "We can't afford it." When my parents were together, I could buy things. Now I can't.
> Predator: Me too. I hate that!
> Child: I waited for six months for the new computer game to come out. My mom promised to buy it for me when it came out. She promised! Now it's out. Can I buy it? Nope. "We don't have enough money!" I hate my mom!
> Predator: Oh! I'm so sorry! I got it! I have this really kewl uncle who buys me things all the time. He's really rich.
> Child: You're sooooo lucky. I wish I had a rich and kewl uncle.
> Predator: Hey! I got an idea! I'll ask my uncle if he'll buy you one too....I told you he's really kewl. I bet he'd say yes.
> Child: Really!? Thanks!!
> Predator: BRB [cybertalk for "be right back"]... I'll go and call him.
> - - -
> Predator: Guess what? He said okay. He's gonna buy you the game!
> Child: Wow, really? Thanks. I can't believe it!!!
> Predator: Where do you live?
> Child: I live in NJ. What about you?
> Predator: I live in New York. So does my uncle. New Jersey isn't far.
> Child: Great!
> Predator: Is there a mall near you? We can meet there.
> Child: Okay. I live near the GSP Mall.
> Predator: I've heard of that. No prob. What about Saturday?
> Child: Kewl.
> Predator: We can go to McDonald's too if you want. We'll meet you there at noon.
> Child: Okay. Where?
> Predator: In front of the computer game store. Oh! My uncle's name is George. He's really kewl.

Child: Great... thanks, I really appreciate it. You're so lucky to have a rich and kewl uncle.

Saturday arrives, and the child goes to the mall and meets an adult outside the computer game store. He identifies himself as "Uncle George" and explains that his nephew is already at the McDonald's waiting for them. The child is uncomfortable, but the uncle walks into the store and buys the $100 game. He comes out and hands it to the child, who is immediately neutralized and delighted. Stranger-danger warnings are not applicable. This isn't a stranger—he's "Uncle George," and if any proof was needed, the computer game is it. He gets into Uncle George's car without hesitation to meet his friend at McDonald's. The rest is reported on the 6 o'clock news.

It's disgusting. It makes us sick to our stomachs, but it happens. Not very often, but often enough that you need to be forewarned. (Several thousand cyberpredator cases are opened each year by law enforcement agents in the United States.) But no matter how often it happens, even once is too often. Knowing how they operate and the tricks of the trade will help us teach our child how to avoid being victimized. Each case differs, but the predators tend to use the same general tactics. Aside from the "bait and switch" scam discussed above, they often attempt to seduce a child. They want the child to "want" them.

The Script—How They Operate Online

They begin by striking up a conversation with the child, trying to create a relationship of trust and friendship. They often masquerade as another child or teenager, typically of the opposite sex, unless the child has indicated homosexual interests. (The child may or may not know the "seducer's" real age by the time they meet face-to-face.) Phone calls usually start at this point. Sometimes gifts are sent to the child as well, which may include a Polaroid camera and film. Once they have broken down barriers of caution, they begin introducing sexual topics gradually, often with the use of child pornography to give the child the impression that other children are regularly involved in sexual activities.

Then they begin to approach the child's own sexuality and curiosity, by asking questions and giving them "assignments," like wearing special underwear, sending sexually suggestive photos of themselves to the pedophile, or performing certain sexual acts. These assignments eventually broaden to the exchange of sexually explicit photographs (using the Polaroid, cell phone camera or digital camera) or videos of the child. Finally, the pedophile attempts to arrange a face-to-face meeting. (He may also have divulged his true age or an age closer to his actual age at this point.)

Why It Works

All the lectures we have given our children from the time they are very young about not talking to strangers aren't applicable online, where everyone is a stranger. A large part of the fun online is talking to people you've never met. In addition, our children's stranger-danger defenses are not triggered when other kids are involved. The warnings apply only to adult strangers, not to other children.

If any of us walked up to a child in a playground and tried to strike up a conversation, they would ignore us and probably run away. But if an unknown eleven-year-old came up to another eleven-year-old in the same playground, they'd be playing in ten seconds flat! That's how the pedophiles get in under our kids' stranger-danger radar—they pretend to be other kids. And children often believe what they read and hear. They "know" things about the predator because they believe what he told them. They also believe what they read about him in his "staged" profile, which supports what he told them. So it's not just true, it's confirmed.

There are many stages at which the pedophile can be thwarted by an observant parent. In addition, children with healthy friendships and a strong, open, and trusting relationship with their parents are less likely to fall victim to pedophiles online. Pedophiles typically prey on a child's loneliness. They feed the child's complaints about her home life—creating an "us-versus-them" atmosphere. "Your mom is so mean to you! I don't know why she won't let you _____." (Fill in the blank with whatever we try and limit: makeup, malls, concerts, etc.)

This atmosphere does two things: It creates a distance between the child and her parents, at the same time bringing the child into a special secret alliance with the pedophile. (You should know that boys are almost as often the victims of Internet sexual exploitation as girls are, but they report it less frequently.)

I have followed many cases over the last few years. In my role as WiredSafety executive director, I've also been responsible for reporting several of these to law enforcement and for helping many families through the pain of prosecution. Sometimes we just help the families survive what the molestation has done to them. (The child isn't the only victim—entire families are torn apart in the aftermath of a molestation.) Parents feel guilty for not having protected their child, siblings don't know how to treat their fellow sibling—the pain can continue for a lifetime, and even more. And, in addition to being hurt physically, the young victim's heart is broken by the betrayal of trust.

Anatomy of a Real and Early Case

One case I reviewed many years ago involved a New Jersey teenager and an Ohio adult predator. It was one of the earliest reported cases of cyber-predatorial conduct, discovered in 1996. Luckily, the liaison was discovered before the girl met the man face-to-face. But it had gone on for a year and a half before being discovered by the girl's mother. As you read the details, think about what could have been done to discover the situation earlier and how you can use these precautions to protect your children.

Paul Brown, Jr., an Ohio resident, was forty-six years old. He was also unemployed, weighed over four hundred pounds, and lived in a basement. He had accounts with several ISPs. Mary (a hypothetical name for the young girl involved) was twelve when her mother, a schoolteacher, bought her a computer, reportedly because Mary was having problems making friends. When she got online, Mary posted a message on an online service, in the spring of 1995, looking for a pen pal. In her message she described herself as a teenage girl. Paul Brown, Jr,. responded to the message, using his real name (something they often do, surprisingly) but identifying himself as a fifteen-year-old boy.

Brown and Mary maintained an e-mail and telephone relationship for several months. As the relationship became more involved, they began writing letters, and Mary sent Brown a photograph. He told her that he was living at home with his mother and was hoping to find a girlfriend. In early August, Brown asked Mary for a "favor." "If I sent you a roll of film, could you get one of your friends to take pictures of you in different outfits and maybe hairstyles? Makeup if you use any, and different poses. Some sexy, if possible. Please. Baby for me. Thanx. You're the best. Love Ya."

Mary complied. For the next eight months, they continued to converse and correspond, and Mary sent additional photos. Brown encouraged her with juvenile antics, such as using stickers in his letters to her saying things like "Getting better all the time!" In May 1996, Brown sent Mary a special love note. "Saying I love you... seems to be an understatement. At the age of 14 you have captured my heart and made it sing... I love everything about you…."

Shortly thereafter, Brown confessed to being in his twenties. He also suggested that Mary videotape herself in sexually provocative poses. She did. After Brown had reviewed her videotape, he returned it to her with instructions to redo the tape and include views of her genitalia and breasts. He later admitted to being divorced and in his thirties. He reportedly also sent her small gifts from time to time.

A few months later, in response to Brown's promise to pass copies of the tape to four members of a rock band Mary admired, she sent additional videotapes to Brown. (Brown told Mary that he knew the band members very well.) Each tape sent to Brown was designated for a different member of the band and contained sexually explicit conduct. Brown apparently had also sent her his size 48 underwear. When her mother discovered the underwear, the authorities were notified. Tracing Brown through phone records, special agents of the FBI in Cleveland seized the videotapes and photos of Mary and of more than ten other teenage girls from across the country.

Mary was fourteen when this was all discovered. Brown pled guilty to enticing a minor to produce sexually explicit photos and videos and was sentenced to a little less than five years in prison (the maximum penalty for a first offense). In a written statement to Brown following all of this, Mary said, "I trusted you. I thought you were my friend."

There are several things that stand out in this case. One, interstate phone calls were made by Mary. Parents should always be reviewing long-distance bills for suspicious calls. Two, Mary was lonely. These kinds of children are often the most vulnerable; a parent should be involved in their online friendships, and monitor their online lives. And, three, as hard as it is to know what our kids are doing when we're not around, especially if you are a single

parent, a year and a half is a long time for a relationship to be going on undiscovered. You should spend time learning who your children's friends are, online and off. But Monday-morning quarterbacking is always easier than playing the game in real time. We may look at the situation and say that could never happen to one of our kids. However, there but for the grace of God go all of us....

Knowing your child is lonely and has problems making friends is the first sign that the child may fall prey to a pedophile or cyber- predator. Predators can spot lonely children. They can also spot kids who are new online and may not yet know all the rules. Most teens, when surveyed, admit to having been propositioned online. But what may be obvious to a cyberstreetsmart kid may not be so obvious to a child not yet familiar with cyberspace. Pedophiles befriend these kids and patiently build trust and a relationship—looking toward the day when they can meet face-to-face.

Encourage your children to make online friends, but learning about their online friends is an important way to avoid these secret relationships. Education is important in avoiding this danger, too. (Had Mary been forewarned about how pedophiles operate online, she may have been more attentive to how old Brown sounded on the phone, and been more aware of his classic tactics.) So is control over incoming and outgoing information when younger children are involved, using technology blockers, monitors, and filters. These kinds of situations can be avoided if you plan ahead, educate and communicate with your children, and keep your eyes open.

Getting in Under Your Radar:

Even when parents are watching, bad things can happen.

I included the Paul Brown case in my first book, A Parents' Guide to the Internet. (He was sentenced in 1997, when I wrote the book.) I included it because it was a good example of how cyberpredators typically operate, and suggested that if the mother had been a bit more attentive, it might have been discovered earlier. I was right about how cyberpredators operate. I was wrong about how being attentive might have avoided the sexual exploitation. It takes more. It takes both an attentive parent and a teenager who has been taught how these pedophiles operate online.

In November 1998, I met a mother who did everything right. She was attentive and inquisitive about her daughter's online relationships. She asked the right questions. She had a good relationship with her daughter, and yet Charles Hatch, a child molester from Utah, got in under everyone's radar and sexually exploited her thirteen-year-old daughter.

Jennifer (not her real name) was eleven and a half when she first met "Charlie" online. She thought he was a few years older, and was intrigued about befriending a slightly older teenage boy. Jennifer was an honors student and had already been taking advanced college courses while still in middle school. She lived in a loving and warm household with her mother and father. She also had siblings and half siblings from her father's previous marriage. They were all close.

Jennifer's mother, Sharry (also not her real name), talked to Jennifer about her online friend, Charlie. She insisted on talking to Charlie himself, by phone, once he and Jennifer had started calling each other. He passed the phone call test, and Sharry was convinced that he really was the teenage boy he professed to be. Either he had manipulated his voice to sound younger or he had a younger person make the call. Charlie even called and spoke to Jennifer's brothers, talking about when he would be their brother-in-law someday, after he and Jennifer were married. He pleaded with Jennifer to come and visit him in Utah. Sharry invited him to visit them instead. But Charlie always had a reason he couldn't come.

As things progressed, Sharry insisted on talking to Charlie's mother. He first avoided it by saying she was sick, later that her sickness had become cancer, and that eventually she died from the cancer. The family fell for this, hook, line, and sinker. Most caring families would. Although the "relationship" progressed for almost two years, it remained relatively tame. Charlie was romantic rather than predatorial, and he sent her expensive gifts, including a Polaroid camera. (Remember the Polaroid camera Paul Brown sent?)

Jennifer was inexperienced with boys and dating, and Charlie seemed to know not to push her too fast. But about a year and a half after they met online, Charlie sent her sexually explicit photos of himself from the neck down. She became very uncomfortable and pulled back. But several tragedies occurred around the same time, which made Jennifer easier prey. Her father was hospitalized with a serious illness, and her sixteen-year-old half brother died of a brain hemorrhage.

Charlie, like all good predators, knew when to strike. He told Jennifer that she owed him sexually explicit photos of herself, since he had sent those of himself. When she refused, he told her that she would be left alone, since her family was dying or would die—and he threatened to leave her. Reluctantly, after fighting against it as hard as she could, she acquiesced and sent him sexually explicit photos of herself.

When Sharry was cleaning Jennifer's room, she discovered a letter in which Charlie had set forth the sexual poses he wanted Jennifer to photograph. Sharry sent him a letter, confronting him. She said that he didn't sound like a teenager in the letter. She told him that if he ever contacted her daughter again, she would inform the police. He never replied, and Jennifer was not permitted to use the Internet for months.

One day, just when Jennifer and Sharry thought that the whole episode was past them, the phone rang. It was a detective from Utah, who informed Sharry that Jennifer's photos had been discovered in Hatch's day planner by a coworker. He wasn't sixteen—he was thirty-six. He was a former teacher who had been dismissed by the school after having been accused by a student of sexual abuse. (The school hadn't taken any other action.) He was currently employed by the welfare office in Utah, and was married with children and step-children.

Six months later, Charles Hatch was convicted of sexual exploitation in a Utah federal court. He began his six-and-a-half year sentence in early June 1999. As a condition of his plea, he will not be permitted to use the Internet. This mother has become a dear friend of mine, after seeking WiredSafety' help in getting through this. She was the first parent to speak out publicly about her child being targeted by a sexual predator online.

Unfortunately, the predators are willing to try many different ploys until one finally works.

Using Celebrity's Names

I was having lunch in Los Angeles with one of my girlfriends when Nick Lachey walked into the restaurant. She pointed him out to me and I immediately grabbed my business card and approached his table (to the utter embarrassment of my friend). I introduced myself and told him I needed his help. I explained that predators were using his name and the name of other celebrities to lure kids into meetings and unsafe activities. They find teens who post their favorite celebrities on their profiles, websites or other online communications. Then they create a profile claiming to be a close personal friend of that celebrity. They offer to forward a pic of the teen to the celebrity, and seek sexier and sexier pics as time goes on, ultimately ending with an offer to introduce the teen to their favorite celebrity in real life. Years ago, Justin Timberlake was the most popular of these celebrity lures. Nick is now. He listened intently and turned white when he realized people where using his name to hurt his young fans. He offered his help.

When I left his table, he has agreed to do a public service announcement to help teens understand that is anyone claims to be a close personal friend of a celebrity, they aren't. Or won't be for long. I was very excited, but not as excited as I was two weeks later when someone from Nick's office called asking me to help them create a safer teen-only social networking site called YFly.com. I agreed and YFly.com became a reality with the financial assistance of Tom Petters (and the Petters Group), and the creativity and energy of its founders, Drew Levin and Daniel Perkins. I joined the team to set up a safer network and create the most advanced educational and awareness content online, just for teen users. The young users can click on "Report the Creep" if they suspect someone is an adult posing as a teen.

It's a beginning. Finding safer technologies and services is part of the solution. So is awareness using teenspeak.

Shannon, one of our Teenangels is 14 years old. She was selected by Teen People as one of the twenty teens who will make a difference. She has gone them one better...she is already making a difference. It is with pride that I

introduce Shannon Sullivan, one of my Teenangels.

Common Internet Sexual Predator Ploys...How it works online

WiredSafety has done a substantial amount of research on how predators operate offline and online. Working with missing children organizations internationally, Internet providers, law enforcement and victims and their families, we have developed a substantial knowledge base about how teens and preteens are lured into offline meetings and online sexual exploitation. From the young victims of sexual predators and online sexual exploitation, we have learned the typical [ploys and how they unfold. By handling online one-to-one help for victims of cybercrime and cyberabuse, we have learned what parents and teens need and how to get them assistance quickly. WiredSafety has stood on the front line against Internet criminals and abusers since 1995.

There are certain tactics that sexual predators use offline to prey on children offline, whether they are strangers or someone known to the child. Interestingly, these same ploys are often used online, by Internet sexual predators, with some “virtual” modifications. Only a few ploys, which are aided by the anonymity of cyberspace, are unique to cyberpredators. Until our recent work, no one has pulled together a list of common predator ploys used by offline sexual predators and compared them with the ploys used by online sexual predators. Our researchers are developing additional materials and studies to expand what we have already learned.

This new research is crucial to keeping our teens and preteens safer. Protecting young people from Internet sexual exploitation is much easier if the young people are aware of the kinds of tricks and ploys used by the predators. If they are alert to possible "ploys" they are less likely to be caught off-guard. Many of these ploys are used over and over again by perpetrators and taught to others within their child molester communities. They include: asking you child for assistance (this is the help me find my puppy ploy, when used offline), the love and affection, confidence and trust ploy (where the child is groomed to fall in love with their online soul mate), the curiosity ploy, the fear tactic, the games and fun, the fun and job offers and the modeling, talent scout or beauty contest ploys.

"Don't talk to strangers" is probably the most common warning parents give their children in an attempt to prevent abduction or exploitation. Unfortunately, these warnings don’t work in cyberspace, where one of its greatest benefits (and the most fun for teens) is being able to communicate with strangers. In addition, unlike the perception of a “stranger” as the raincoat clad, dirty, bearded man who lurks on street corners or in playground, Internet “strangers” quickly become Internet “friends” and the stranger danger radar is no longer working. The kids, tweens and teens are no longer treating them with care, and have let them into their inner-circle. That’s where the real dangers begin. These child molesters can get in under your and our children's stranger danger radar.

Sometimes this happens because they believe their net friend is another young person. And a “stranger” is never another young person. Unlike the offline counterpart ploys, a 47 year old can easily masquerade as a 13 year old online. Or someone can be three or four different people at the same time online, engaging in conversations with themselves in a public setting, allowing young by-standers to think they are trustworthy, or famous or otherwise worth talking to. Online our children are in the dark, literally.

With the number of young sexual predator victims growing, and the amount of contact information young people are sharing online in blogs, profiles and away messages putting them at greater risk, awareness and prevention in these areas is crucial. Partnerships with Internet service providers, media and entertainment companies and learning from and sharing what we know with each other is what needs to be done. And, it is worth the effort. Our children are entitled to sleep more safely at night, and enjoy the wonders of the Internet...without fear of being preyed upon or hurt.

Parents are the Beginning

From the time I published my first book for parents on Internet safety in 1997 (*A Parents Guide to the Internet)* we have been educating parents on how they can stay ahead (or at least on par :-)) with their children and teens online. Our quick guide - Parenting Online, is available online without charge and has been copied and distributed by hundreds of groups and schools around the United States. It includes a parent/child contract, a quick guide to parental control technologies and our very popular "Common Sense to Cybersense." (A copy of this guide is attached as part of the Parenting Online Guide.)

Now, many parents want something quick. They are happy that expert groups such as WiredSafety.org understand all the issues and that they can turn to us. But they are being pulled in so many directions just by virtue of their parenthood, that they want "Just the Facts...Madam." Our new programs, called Internet Safety 1-2-3 make it easy for parents to spot the risks by age, and also by technology. Our new automated Family Internet Safety Plan works using this new approach (patent pending) to help parents understand what works for them and what things they need to do to keep their family safer, given the technologies they use, the ages of their children and their value system. (A quick example of the kinds of things covered is attached as an Appendix 3 in our "Cheatsheet on Risks by Age".)

Our children are worth it, and so is the Internet. Too often blamed for everything from the Black Plague to the sinking of the Titanic, the Internet is a wonderful tool for learning, communication and entertainment. It levels the playing field between the haves and the have-nots. All children look alike online. No one is classified by their race, ethnic origin, religion, accent or physical ability. Online they are all just children. And like it or not, the Internet is here to stay.

We're all in this together. Let's work together to make the Internet fun, safe, private and educational for children. And let's work together to make sure that the children's Internet industry, which has so much to offer our children, flourishes!

For the children.

I remain willing to help, and provide input and expertise in any way this Subcommittee can use my help and expertise.

I wish to thank the Subcommittee, its chairman and all its members for inviting me to present this testimony on such an important subject.

Parry Aftab, Esq.

APPENDIXES:

Appendix 1: WiredSafety's Guide to MySpace.com

This was posted on MySpace.com as a public service from June 2005 to help parents understand how to keep their children safer on the site.

(a 501c-3 corporation)

WiredSafety's Guide to MySpace.com

Hi! My name is Parry Aftab.

I am an Internet privacy and security lawyer and founded and run the world's largest online safety and help group, WiredSafety.org. You may have seen us on TV or read about us in magazines or newspapers on Internet safety issues for every member of the family. We specialize in helping protect kids and teens online. We also have extensive information for adults on Internet safety, privacy and how to avoid becoming the victim of identity theft, cybercrime or cyberabuse. And are the leading resource for parents on Internet safety.

We are posting this information and our guides and other materials available to help MySpace users as a public service. We are not employed by or legally affiliated with MySpace. We are an independent charity devoted to helping everyone stay safer online. And MySpace is serious about trying to help their users be safer online. That's why we have agreed to make our materials available at MySpace and provide special help for MySpace users and parents of MySpace users.

It's a challenge protecting privacy and personal information while building a blog or profile page no matter how old you are. But there are some tricks and tips WiredSafety.org has pulled together over the years that might help you stay safer while letting you express yourself on MySpace.com. To learn how to protect yourself better online, read our MySpace.com Safety Guide and other safety tips at WiredSafety.org.

For Parents: Recently, I have been receiving a large number of inquiries from schools, parents, regulators and the media about social-networking websites. I decided that it was important to address parent concerns and answer their questions. Where better to do that than on the most popular of all social-networking sites, MySpace.com?

MySpace.com and other similar sites are designed to allow people to share their creativity, pictures, and information with others. It also allows them to network with others online.

Sometimes people do this to find romance. Sometimes they do it to find friends with similar interests. While this may be okay for adults, it is not okay for kids.

MySpace.com recognizes this, and prohibits anyone less than 14 years of age from using their website. There are special rules and settings for teens between the ages of 14 and 16 too. These rules and settings are designed to help these younger teens better protect their privacy and be safer on our site. You can learn more about these settings at WiredSafety.org and at MySpace.

Unfortunately, while MySpace has set rules to keep preteens and younger teens off the site, they can't prevent kids from lying about their age and pretending to be 14 years of age or older. To address this, MySpace.com has developed methods designed to help identify preteen members by reviewing certain content of member profiles. It doesn't review their photos to determine if the person appears to be younger than their stated age, but can scan the profiles looking for certain words and statements that can often give away the young person's real age. It's not perfect, but it does help spot many underage members. Thousands have been removed from the site for having misstated their age. And I expect that thousands more will have their profiles deleted in the months to come.

MySpace.com really does try to keep them off their site. Many other similar sites do not. That's why we agreed to post our safety information there. They care and are working hard to keep the site as safe as possible. That matters to us at WiredSafety.org. If your teens are going to lie about their age and post a profile somewhere online, I would prefer it's at a site that cares about their users and is willing to work with an online safety group, rather than one that doesn't care or seem to care at all.

But no matter how much they may care about the safety of their users, some parents are shocked about what their teens are posting online and the things they admit to have done offline. And a shocked parent (or a frightened one) is often an angry one. Before you do anything else, take a breath. Think about how your parents would have reacted if they had been able to record everything we said and did with our friends, when we thought they weren't around. I would still be grounded, trust me!

Then, take another breath. Make a cup of coffee or tea and prepare to handle a tough parental choice. (I know, all are tough ones these days, but this one is especially challenging.)

Have you seen their page yet? If not do you know how to find it? You should start by asking your teen to show it to you. If they refuse, or you want to see it before you confront them, you can search for it easily. You can learn how at WiredSafety.org.

If you discover that your child is posing as someone older and using their site, you have two choices. You can have the site taken down, or you can supervise what they are posting and doing at MySpace.com. It's important to all parties that you help maintain your child's safety while online. Unfortunately, while we at WiredSafety.org can help you keep yourself and your family safer online, we can't do your job for you. We need your help.

For parents, the procedures for deletion of an underage MySpace account fall into the following two primary categories. No matter which one applies in your case, you should take advantage of this opportunity to review their page first. You might be surprised (hopefully pleasantly).

If they haven't posted anything to put them at risk, and aren't communicating with strangers, ask them why they want a page at MySpace.com. You might be surprised at what they tell you. While parents freak out (understandably) at the provocative images and wild language used by many on MySpace (even though they violate the site terms of service rules), most of the teens don't see them or pay attention to them.

Believe it or not, they are there to show off their creativity and self-expression and to communicate with their offline friends. As long as they are old enough to understand the rules and adhere to them (no one under 13 is old enough for this, even with parental approval in my humble opinion), and as long as you keep an eye on what they are doing, posting and how they are communicating with others, it's YOUR choice as to whether they keep their site up or not. (Make sure that you don't become the self-appointed MySpace.com police, reporting other people's kids for posting underage until you speak with their parents first!)

If you find that they are saying and posting inappropriate things or those comments don't seem to conform to their otherwise good offline behavior, don't panic yet. Think about how our parents would have reacted if they could have seen or heard everything we said to our friends when no adult was around. I guarantee that they would have been almost as shocked as many parents are about what their kids are posting online. Also, remember that many of the things your kids are saying are being said to impress their audience and are often not true. (Luckily!)

The important difference between what we used to say or do and their posting online, however, is that when we acted out or boasted about acting out, we didn't do it to an audience of millions of people (including our parents, principals and everyone else). So, while you shouldn't panic, you should take quick action if your kids are posting personal information in a public forum, such as MySpace.com, or communicating with strangers online. Either have them remove the personal information and use a photo software program to alter their pictures (to a pixilated, cartoon or sketched form that can't be misused by others or used to identify your child offline) or have them take down their profile page entirely. (Note that if you overreact they will just rebuild another one tomorrow at MySpace or another site.)

You can learn more about how to help them surf and communicate safely at WiredSafety.org, WiredKids.org or Teenangels.org. If you fear that they are communicating with strangers, or even thinking about meeting them offline report it right away to the authorities or to the cybertipline.com. We are building a new page just for kids on sexual predators - Katiesplace.org. Victims of Internet sexual predators are helping us explain the real risks in terms the kids can understand. This is up, and growing (it will always be under construction, we hope, improving as we add more and more features and content.) Then you can send them to KatiesPlace.org to learn how Internet predators operate. It may help scare them safe. If you fear that they are being cyberbullied, check out our Stopcyberbullying.org page, or reach out to WiredSafety.org's cyberbullying help line.

With that being said, here's how you can have their page taken down from MySpace.com:

Taking Down Your Child's Profile Page:

There are two ways to have their pages taken down, or everything on them deleted. You can do it the easy way (with your child's cooperation) or the hard way (without their cooperation). Even if they are cooperative, though, their friend may have set up their account using a fake e-mail address, or they may have used a fake e-mail address, or they

could have forgotten their password or their friend never gave it to them. These may require you use the Alternate Account Closure Process, below.

If your child has their password and is cooperative, and used a real e-mail address when setting up their account:

First try asking your child to take it down themselves. They have a password for their page that can be used to remove anything (or everything) from their page. Tell them to use it to wipe their page clean of any content or contact information. Then you can move forward to remove the entire profile or not. Since the page will be entirely blank, it won't make any difference if it remains up.

If you want to go through the bother to take down the empty profile page, this is how you do it:

- Logon to MySpace

- Click "Account Settings"

- On the "Change Account Settings" page, click on "-**Cancel Account**-"

- Click on the "**Cancel My Account**" button in the confirmation box.

- Include remarks if desired; then click on the second "**Cancel My Account**" button to complete the request process.

- A cancellation message will be sent to the email address of record. Replying to this email **is required** in order to complete the automated account closure process.

Note: if you child lied about their e-mail address when setting up the account (see, they do know something about protecting their privacy ☺), this won't work. The e-mail with the automated process link has to be received and replied to. So, even if your child is cooperative, you'll need to follow the instructions to remove a page if the e-mail address used to set up the account is not operational. It may not be worth it if you followed my advice and removed everything on their page anyway.

Note that many ISPs and e-mail providers block MySpace communications, thinking they are spam. So, when they send the instructions, they might not get through. If that happens, you should use the method set out below that we helped MySpace create.

Alternative Account Closure Process:

If your child is cooperative and had their password, but used a fake e-mail address or someone else's e-mail address when setting up the account; or

If your child claims not to know their password or lied about the e-mail address when setting up the account, or is uncooperative

Unfortunately, in addition to lying about their age, many kids will use a bogus e-mail address when applying for membership, or may profess to have (or really have) forgotten their passwords. Often friends set up profile pages for their close friends and use a fake e-mail address or never turn over the password. These circumstances can make it virtually impossible to use the process outlined above.

MySpace recognizes this reality and has established special account cancellation procedures to deal with these contingencies. (These are unfortunately required as many teens cyberbully and harass each other, notifying MySpace.com to delete a profile while posing as the parent of their victim.) When a parent wishes to close an underage account and either the child is uncooperative, or a technical difficulty precludes the use of the general account closure method, the following procedures can be used.

If they know their password but don't have a real e-mail address or can't remember it, have them remove everything from their account, leaving a blank page, except for typing in "remove this profile" somewhere on the page. Then notify MySpace.com's customer service staff giving them the exact url of your child's profile (what appears in the window of your web browser when you are viewing their page (cut and exactly copy it into the e-mail). Ask them to remove the profile and let them know it is blank and has a posted instruction to remove it. This let's the customer service staff know that it is an authorized removal. As lone as you have given them the right url and the message appears on the profile, the profile page will be removed as quickly as possible.

If your child does not have their password, or claims not to have it, it's a bit more complicated. First contact MySpace.com's customer service staff at customercare@myspace.com. This request HAS TO include your child's URL address in the form. It is the address that appears in your browser window when you access their profile page. It starts with "www.myspace.com/" and will include numbers that identify their own profile page. (For example, an address could be www.myspace.com/123456.) This information can also be located on the left-hand side of the Welcome page that is displayed following your child's initial logon.

When MySpace.com's help staff receives your e-mail, assuming your child's profile is included in the email, the site will review the account for any definite indications that the account owner is underage. If definite proof IS found, the child's profile WILL be removed and an email will be sent to the email address on the account explaining WHY the account was deleted.

If the child's URL is NOT indicated in the cancellation request, the parent is emailed with a request for the information.

While all parents should work WITH the child in removing the account through normal cancellation procedures discussed above, if the child does not have their password or claims not to have their password, the parent must submit an affidavit stating that they are the custodial parent or legal guardian of the child, the birthdate of the child, that they want their child's profile removed and that their child does not have the password to remove their profile information or has used a fake e-mail address and therefore cannot use the normal account closure procedure, and providing offline contact information. E-mail customercare@myspace.com for an address to mail it. The MySpace.com personnel will then contact the parent or legal guardian by phone number in order to confirm the custodial parental or legal guardian status of the requestor. Upon successful verification, the minor's account will be removed while on the phone with the parent or legal guardian.

If schools need help with one of their students, there are special e-mail addresses set up just for school administrators. And with our help, MySpace has adopted the most liberal law enforcement policy online. If their users is at risk, they want law enforcement to have the information and access they need to protect them. They have hired a law enforcement liaison to help law enforcement agencies and have published a law enforcement

investigators guide, which we helped write.

While MySpace.com is doing its best to keep your children from using their website and lying about their age, it's up to parents to do their job too. Parents need to talk with their children about not sharing personal information online. Personal information includes pictures, names and addresses, schools they attend, cell and phone numbers and many other less obvious things, such as the name of their school team, ethnic background and even a mall near your house. (You can learn more about how to talk to your kids and what you should be asking at WiredKids.org or WiredSafety.org.

We are developing a special program just for parents concerned about their kids using social-networking and online dating sites. It will teach you what you need to know about finding out if your child has a profile on one of these sites, how to review them and remove them, if you want to. It will also help if your child is being cyberbullied by other members from these sites, or is cyberbullying others.

The best way to find out if your child has a profile on this or another similar site is to ask them. If you're not sure that your child is being honest with you, you can search MySpace.com using their e-mail address, or by searching for their school. (You click on "search" and enter their email address or full name in the appropriate search box.) If you find that your child has a profile on the website, you should review it. It's amazing how much you can learn about your child by reading their profiles. Does it contain personal information, such as their full name, address or phone numbers? Has your child posted photos? Are they photos of themselves or someone else? Are they sharing poems they write or provocative comments about themselves or others?

Ultimately, protecting your child is your job. We will be building a few tutorials at WiredSafety.org and at MySpace.com to help parents and their children understand how to be careful when communicating publicly online.

Ask them why they created the profile. You might learn that they wanted to share their thoughts with others, make new friends or even allow others in their school to get to know them better. But not all of their motives are as noble or safe. Some may be interested in meeting new romantic interests or role-playing inappropriately online. And when a young preteen lies about their age posing as a seventeen year old at the site, that can be a serious problem. Others in their late teens might approach your child thinking they were older. That's bad for everyone.

If you discover that your child is posting provocative comments or inappropriate images online, it's time for the tough talk. The one about stranger dangers and how that cute eighteen year old boy they meet online may not be cute, may not be eighteen and may not be a boy. (Parents of young boys need to understand that their children are equally at risk. About one-third of the cases of Internet sexual exploitation are men exploiting boys.) Our children need to realize that there are real risks relating to meeting strangers offline, including murder. The first confirmed murder victim by an Internet sexual predator was thirteen when she died, three years ago May 2005. The risks are real, not matter how smart, sophisticated or tech savvy your kids are. We recommend the book, A Girl's Life Online, by Katie Tarbox. We are also developing a few videos for teens teaching them about standard ploys used by Internet sexual predators to lure a young boy or girl into an offline meeting or sexual exploitation situations online.

It's not easy raising children anymore. It is even harder when the parent is expected to be

expert in Internet, cell phone and interactive game risks. The good thing is that you're not facing these challenges alone. We're here to help.

Just remember that while your kids may know more than you do about technology, you know more about life. And you are allowed to set the rules and enforce them. You're still the parent! There is software you can install that will record what your kids say and post online. There is even one that will e-mail you reports at work. The ones I like best are made by Spectorsoft, and can be found at software4parents.com or spectorsoft.com. But don't use them just to spy on your kids. Treat them like a security video camera in the corner of a bank. No one views the tapes unless and until there is a break-in. Do the same here. Check the program reports if something goes wrong. It will collect whatever you need for evidence and to help your child if something goes wrong.

Also, check your parental control programs. Many, such as AOL's and MSN's, can block access to social-networking websites or other sites you think are inappropriate for your younger child. There are many other products you can purchase to block sites as well. (Check out software4parents.com to learn about and purchase some of these.) Just remember that the best filter is the one between your children's ears.

If you child is being bullied by another MySpace.com user online, check the terms of service first. If the bullying violates MySpace.com's terms of service, report it to TOS and the offending comments and/or profile will be removed. If something serious occurs and you need to reach out to law enforcement, let them know that MySpace.com has created a special procedure for law enforcement inquiries, especially when the safety and well-being of its site users is involved. They should contact abuse@myspace.com. Cyberbullying is a growing problem. You can learn more about it, as well as how to prevent and handle cyberbullying incidents, at WiredSafety's StopCyberbullying.org and InternetSuperheroes.org. WiredSafety.org also has a reportline link for victims of cyberbullying, their schools and parents where specially-trained volunteers assist victims of cyberstalking, harassment and cyberbullying without charge.

If schools are looking for a presentation or program to address their students' posting inappropriate profiles or using these websites while underage or other parent concerns, they should visit WiredSafety.org, WiredKids.org or Teenangels.org. Schools may find many of their students using a particular website. Working together with schools and parents, we may be able to keep our kids off of website that are inappropriate for young children and teach them to make good choices online and offline.

If you have other questions, contact me at askparry@wiredsafety.org.

Stay safe.

Parry Aftab, Esq.
Executive Director,
WiredSafety.org (wiredsafety.org)
The world's largest Internet safety and help group

Learn more about WiredSafety.org!

Appendix 2: Parry Aftab Bio and CV

Contact Info:

Dr. Parry Aftab
Parry@Aftab.com
www.aftab.com
+1-201-463-8663

Introduction:

Parry Aftab was one of the first lawyers to practice Internet law. Known for her ability to think outside the box, she quickly became a leader in the emerging area of Internet law and policy. She now devotes most of her time to issues impacting children and families online. Dr. Aftab is the award-winning "Privacy Lawyer" columnist for Information Week magazine. She is a frequent expert resource for and quoted by most leading media outlets, online and offline, around the world. Dr. Aftab is a sought-after public speaker and the author of several books. When Internet policy and consumers and families online are involved, hers is the first name mentioned.

About Parry:

Parry Aftab resides in the NY metropolitan area. She started out on Wall Street in 1984, as a corporate takeover lawyer. Along the way, she completed her undergraduate degree in less than 2 years, as Valedictorian, with her two children in tow. She is a member of *Phi Beta Kappa* and an NYU Law School graduate with a *juris doctorate* degree. Her work with children online began following a CNN appearance on Internet censorship in 1997. She founded and runs the world's largest Internet safety group and works closely with law enforcement, the Internet industry and governmental agencies around the world. Dr. Aftab has received many awards for her work.

Areas of Expertise:

Parry Aftab is a legal expert in all aspects of best practices and cybercrime and abuse. She has advised the Internet industry on consumer and children's issues since 1994 and is called the "Kids Internet Lawyer." Dr. Aftab expanded her focus to privacy and security law and the application of sound practices to new interactive technologies.. Her expertise now extends to interactive gaming, mobile and wireless technologies, as well as the Internet. Unlike many experts, Dr. Aftab's talents include her ability to factor in societal, values and legal differences around the world. This enables a truly globally sensitive approach to a global medium.

Additional Information:

Her first book, *A Parents' Guide to the Internet...and how to protect your children in cyberspace*, was released in December 1997. It was a guide for the "technology challenged" parents providing practical solutions to parents' concerns about Internet safety. Her second book, *The Parent's Guide to Protecting Your Children in Cyberspace,* was published by McGraw-Hill and released in 2000 in the United States. It was subsequently adapted for the UK, Singapore and the US Spanish-speaking market. Her third book on Internet safety was written expressly for families in China. It was released in November 2004, in Chinese. Her latest book is a shorter and updated version of her second book, written exclusively for Spain and Spanish-speaking South and Central American families. Her second book, even out-of-date and out-of-print, it is still considered the leading resource for parents on Internet safety for their children. Ms. Aftab reacquired the rights to that book and will be making sections of it available without charge at WiredSafety's website.

Although her vocation was Internet security and privacy law, her avocation is children online – helping them become good cybercitizens and keeping them safe, private and secure online. She is dedicated to helping curb Internet-related crimes against children and assisting law enforcement in bringing the child predators to justice. Everyone who encounters Ms. Aftab is impressed with her passion and energy when children's Internet issues are involved. She has devoted all of her money and time to these issues, since stumbling on an Internet image of a 3-1/2 year old girl being raped online. Ms. Aftab defines that moment graphically as "a branding iron being applied to your brain. It leaves a permanent and painful memory. It stays with you forever."

While her passion is for protecting children from Internet sexual exploitation, she is also devoted to empowering them through access to the wonders of the Internet. She hopes to help all children become better informed and responsible cybercitizens, controlling the technologies instead of being controlled by them. Her programs are designed to teach them safe, private and responsible technology use, which includes teaching them good netiquette and respect for each other and the rights of others, including intellectual property rights of the music, movie, gaming and software industries.

Her newest project, Peers2Peers (peers2peers.org) is designed to teach children and teens to understand and respect intellectual property rights, whether to music, software, games, movies or trademarks. Understanding that the fastest way to stop wholesale piracy) especially of motion pictures) is to teach the children to pay for what they download, Ms. Aftab has combined forces with some of the key players in the IP markets, including major artists, Marvel Comics, multimedia lawyers, software manufacturers, game designers and members of the motion picture industry to help teach kids that everyone has a stake in protecting the legal rights of others. The Peers2Peers program includes classroom lesson plans and curricula, videos and public service announcements as well as a competition where youth volunteers can design their own public service awareness campaigns.

Ms. Aftab was among the first in the world to devote her talents to keeping children safe online. She has helped design programs for parents and children in a wide range of Internet-related issues since 1997, including the P.I.E. Program (Parent Internet Education) for the Baltimore County School system. This was the first of its kind, in educating parents and families about safe and fun online use. She is also an expert on filtering and blocking products. And now provides best practices guidance (in her role as head of the charity) to most of the social networking sites online, around the world.

Her work has been recognized by leading technology influencers, such as Family PC Magazine, when she was awarded Internet Pioneer of the Year in 2001. And child protection agencies have recognized her as well, when Child Abuse Prevention Services presented her with their 20th anniversary Community Leadership Award in 2005. (Past recipients of this award include Senator Clinton, Linda Fairstein, Judy Collins, Dr. Joyce Brothers and the "God Squad.")

Parry Aftab also provides parent Internet education and online safety content for such diverse sites as Nickelodeon, Children's Television Workshop, Disney, Microsoft, AOL, AT&T and MSNBC. She is a regular keynote speaker, and resource on camera for the media on diverse cybercrime, safety, privacy and cyberlaw issues. Recently she became The Privacy Lawyer columnist for Information Week Magazine where she writes on a range of topics that affect technology, policy and privacy. Her expertise is especially in demand on children's Internet issues, because no one knows more about children online than Parry Aftab.

While she is devoted to protecting children online, Ms. Aftab seeks to empower children and their parents, not the censors. Her common sense approach to technology risks and solutions works as well anywhere in the world as it does in the United States. But what really makes her special is her ability to tap into the caring and creativity of young people to craft solutions that are written in their language and designed for their needs.

She is a frequent and respected resource for news programming and print journalists around the world. Her expertise has been featured nationally and internationally in online and print publications, including Readers Digest, Playboy, TV Guide Magazine, Cosmopolitan, People Magazine, Redbook, Biography, USA Today, Information Week, Working Women, Teen People, U.S. News & World Report, Family Circle, Newsweek, Ladies Home Journal, Smart Money Magazine, PC Magazine, Good Housekeeping, Better Homes & Gardens, Family PC Magazine, Yahoo! Internet Life, Information Week, CIO Magazine, The Wall Street Journal, The New York Times, The LA Times, most regional newspapers in the United States, The London Times Magazine, The Strait Times (Singapore), The South China Morning Post Sunday Magazine (Hong Kong), and more. As a result of her work online with children, Ms. Aftab was selected as a charter member of Children Television Workshop's Advisory Board, as well as appointed to The

National Urban League's Technology Advisory Committee. In 2003 she was elected to TRUSTe's Board of Directors. She served on the advisory board for the Ad Council for two terms.

Parry Aftab has spoken to many governmental agencies and groups worldwide, conducted briefings for the U.S. Senate, been a key speaker at the White House Summit on Online Content, the sole Internet-related expert speaking at the 2002 White House summit on Missing and Exploited Children and testified before leading legislative committees and The House of Lords, all with the same message: The Internet is a wonderful resource for families, and once parents understand the online risks, they can use common sense (and perhaps some filtering tools) to help their children enjoy cyberspace safely.

As one of the first lawyers in the world to specialize in Internet legal issues, Parry Aftab is admitted to practice law in New York and New Jersey. She attended law school at NYU School of Law where she received her J.D. degree. She received her B.A. degree as *Valedictorian* of Hunter College (having completed her full undergraduate degree in less than two years), where she was inducted into *Phi Beta Kappa*.

She resides in the New York metropolitan area and is a mother of two. Ms. Aftab can be reached at Parry@Aftab.com.

Parry Aftab

Professional Curriculum Vitae

Phone: 201-463-8663
parry@aftab.com

Internet privacy and security lawyer, licensed to practice law in NY and NJ,
The Privacy Lawyer columnist, author, consultant and public speaker

AREAS OF EXPERTISE: Worldwide Cybercrime Protection and Prevention/Identity Theft/ Privacy, Data Collection and Security / Workplace Risk Management and Security/ Consumer Protection, Advertising and the Internet / E-Commerce/ Cyberstalking and Harassment/ Child Exploitation and Child Pornography, Children Online, Online Marketing, Cyber-workplace issues, Privacy training and coaching

---

CURRENT POSITIONS

President/CEO - Aftab Cyber-Consulting
Executive Director, WiredSafety.org (a 501c-3 corporation)
The Privacy Lawyer columnist for Information Week

EDUCATION

City University of New York — B.A., 1981
Hunter College — *Valedictorian*
(Completed 4 yr degree in 2 yrs) — *Phi Beta Kappa* (Nu Chapter)

New York University — J.D., 1984
School of Law

SELECT HONORS

Community Leadership Award, 2005
Awarded by Child Abuse Prevention Services

American Society of Business Publication Editors Award "Gold" O*riginal Web Commentary*
Informationweek.com for Parry Aftab's
"Patriotism, Compliance and Confidentiality" article

Activist of the Year Award, 2002
Awarded by Media Ecology Association

Internet Pioneer of the Year, 2001
Awarded by Family PC Magazine

Home Office, U.K.
Child Protection, Criminal Laws and Law Enforcement Task Forces

ORGANIZATIONS

TRUSTe
Member- Board of Directors (Elected December 2002)

Ad Council
Advisory Committee member (1999 - 2003)

Children's Television Workshop Online (Sesame Workshop)
Advisory Board (appointed 1998)

UNESCO
President, U.S. National Action Committee, Innocence in Danger (appointed 1999)

Appendix 3: From Parry's Upcoming Book, Internet Safety 1-2-3:

Internet Safety 1-2-3: The Quick Guide

While you can take the time to do your own inventory on risks, not everyone will. This will give you a quick guide on the risks that most children and teens face at certain ages. Read the description of their activities, not just the age ranges. How they are using the technologies and which they are using are more important that their age in determining the risks they face. This can be very helpful when you want to know where to start. Reviewing these will help you know what to look for, especially when you want some quick help. Remember the 3Cs and look for "content" issues, "commercial" issues and "contact" issues. In the early years, though, no matter how you feel about commercialism, most of the quality and fun content and online activities come from the big entertainment companies and trusted family brands, such as Disney, Children's Television Workshop, Nickelodeon and Scholastic.

Under 8 years of age:
The children are lap-surfing and just beginning to use the Internet. Some are pre-readers, and others are new writers and slower readers. That means they can easily make a mistake when typing in their favorite website name or searching for their favorite topics in a search engine. Most are not using interactive communication technologies (e-mail, instant messaging, etc.) without parental screening and supervision. They may or may not be allowed to access the Web without their parents standing over their shoulder. These children play lots of games, online and offline, but most of the ones they play are not interactive (meaning, they don't usually involve them playing against other people). They spend most of their time on favorite sites that usually involve their favorite offline and television characters and brands, such as Disney, Children's Television Workshop, Nickelodeon and Cartoon Network.

Children under eight years of age are very concerned about doing something to break the computer (downloading viruses and spyware applications). It's a good age to get them started with secure surfing and using an anti-virus program if downloading anything or accepting any attachments. It's also a good time to get them to start using spyware and pop-up blockers (perhaps by using a customized toolbar, such as Google's or Yahoo's). They are not yet involved with stranger communication or the risks of meeting people offline.

They need to learn good netiquette and how to respect others online. (I have a written an entire chapter on this called "Ms. Parry's Guide to Netiquette." Pay special attention to this chapter.) They also need to learn how to find new sites without risking full-sized search engines. Being able to communicate with large numbers of friends and have them be able to reach you are less of a problem at this age. The most restrictive parental control technologies work well here. They don't need millions of websites to do their homework at this age. It's less about opening up their access and more about limiting it.

Some children of this age are using mobile phones and handheld gaming devices with networking capability, but most aren't. Prepaid calling cards for their mobile phones are a good decision, to keep them from running up high phone bills. Text-messaging shouldn't be permitted at this age. And the most restrictive settings for all networked handheld technologies is your best bet, if you buy them at all.

And if you are allowing them to play video games, check the ratings and choose one that is appropriate in violence, language and sexual content for your child. Check and make sure that they can't install new video games on their mobile phones without your approval. Keep them from using any interactive game devices, such as X-Box Live or Sony PlayStation Network, or other voice chat games or devices.

Less is more when you are dealing with children of this age. They still believe that their parents are in charge, know everything and are there to protect them. (It's a magical age…Enjoy it, it won't last! ☺) Also, are you using babysitters? Remember what I suggested about password protection and turning off the Internet when you are not home.

- Use filtering or parental control technologies. Block everything that isn't pre-approved, rather than just filtering out the "bad" sites.
- Think about whether they really need e-mail or IM, and if you determine they do, block all

communications from anyone other than pre-approved senders.
- Make sure that the buddy list is no longer than the age of the child, and that you know (in real life) everyone on it.
- Bookmark their favorite websites so they won't mistype them and end up at a "bad" site.
- Use kid-sized search engines: Yahooligans and Ask Jeeves for Kids.
- Limit their online time to no more than ½ hour a day, unless they have a special project for school.
- Check with their teachers and librarians for suggested websites and for recommendations for good resources online.
- Don't let them use interactive games, such as X-Box Live or Sony PlayStation Network yet. You should use our safe gaming award winning Disney's Toontown.com instead.
- Sit down with them as often as possible and find out where they go online, what they like and ask or answer any questions they may have.
- Don't allow them to set up websites, profiles, blogs or away messages or use other public posts without your direct supervision.
- Control their passwords.
- Look for safe site lists you can trust. Check out WiredKids.org approved safe sites list and the other safe sites listed in my "Green Light" section.

From 8 to 10 years of age:
They are beginning to use instant messaging, e-mail and other interactive communication tools. They are also surfing more and spending more time online. They need to learn more about what information they can and can't share with others online, how to choose their passwords and with whom they can be shared. (Parents tend to worry most at this age, as their children do from surfing to communication tools.)

They may be engaged in interactive gaming (playing against strangers, sometimes with voice chat), spending more time playing video games (including more violent and adult-themed games) and be more likely to use adult-sized search engines to find the sites they are looking for. Because of their visiting gaming related websites, like code and cheat sites (to improve their game play), they are prime targets for spyware. And as they learn to flex their cyber-muscles, they are often cyberbullied or cyberbullying others and frequently hacking into, and sending malicious codes to, each other.

Fortunately, they are still too young to be engaged in face-to-face meetings with adults offline, and generally not looking for sexually-explicit content online. They are more interested in finding gory and shocking websites, where baby seals are being clubbed to death.

They often begin to use lewd and inappropriate language at this age too, even if they would never dream of doing this offline. Boys and girls are very different in how they use the technology at this age, as well. Boys tend to be less involved with interactive communications, even with their friends, and girls tend to surf less, spending more of their time chatting or IMing their offline friends. The people they talk with online are still the ones they know in real life. And more have mobile phones, but still need to have prepaid calling plans and restrictions on who can call them and who they can call.

Children begin to register at websites and fill out online forms at this age. Parents need to talk with them about what they can and can't do and which sites to trust. And their homework may require more websites than they can get with the most restrictive parental control settings or with some of the child-sized search engines.

Most of the children in this age group aren't downloading music or other copyrighted media online yet, unless they have older siblings. And they are still willing to tell their parents what they are doing online and when things go wrong online. Parents are still the "good guys" and are an important influence on their online activities. This may be your last chance to have an affect on their online activities. Don't waste it.

- Raise the bar on filtering or parental control technologies if you find they are complaining or are locked out of school-recommended sites. Or make sure that you use a product that will send you an e-mail at work to let you unblock a particular site. (MSN has this feature.)
- If you add IM or e-mail, make sure only pre-approved senders can send your child an IM or e-mail. Consider using a free web-based service with parental controls and spam blockers. That way, whatever they access online won't pollute their real e-mail address, or yours.
- Use a pop-up blocker or toolbar (like Google's or Yahoo's), an antivirus program and a spyware

blocker and remover (this begins the age of dangerous downloads).
- Keep using the Yahooligans! and Ask Jeeves for Kids search engines.
- Make sure that they understand what information can and can't be shared online with anyone.
- Practice chatting online with them so they know how to handle strangers they encounter online.
- Make sure that they know not to cyberbully someone or say or do anything online that they wouldn't do offline.
- Make sure they know how to use the "notify" or "warning" buttons, or consider using a monitoring software to be able to review what they are saying and doing.
- Watch for hacking, password and identity theft at this age. This is when they start stealing each others' passwords and locking them out of their own accounts.
- Also watch for their corrupting your files on your computer with spyware, etc. Back everything up!
- Limit online time (aside from special school projects) to under an hour a day (including all IM and text-messaging time).

Between 10 and 12 years of age:
Cyberbullying is very common at this age. So are filling out forms, signing up for newsletters and registering for contests and giveaways online. More of the children at this age have mobile phones, which should still have a prepaid calling plan and restrictions on who can call them and who they can call. Many have text-messaging on their mobile phones, and if you don't use a prepaid plan, you may find yourself with very high mobile phone bills for their text-messaging use alone.

Some preteens are setting up profiles on social networking websites at this age, usually hiding them from their parents. They are more interested in communicating with their friends from school on these sites, and self-expression and being creative by creating "pink, pink, pink" profiles (how one of my Teenangels described her site). They are still usually chatting and IMing only people they know offline.

But some are starting to feel more confident and are willing to respond to a stranger's message or to engage in communications with a friend of a friend. (A sexual predator will often befriend one preteen to get to their friends.) And some of the younger Internet sexual predator victims engage in meeting strangers offline at this age. They usually think they are meeting a cute fourteen-year-old, but know it's someone they don't know in real life. A much higher portion of victims at this age are female than male.

Some of the boys may begin to seek out sexually-explicit content online. Many of the boys and girls are using lewd language and pretending to be more sophisticated than they are. "Cybersex" or ask the kids call it "cybering" usually begins at this age too. It is when they type sexual things online with someone else (similar to having "phone sex"). Sometimes they don't appreciate the seriousness of what they are doing, but do it anyway. Sharing their personal information and communicating with strangers are the most important issues they face at this age. Keeping them grounded at this age will payoff in the future. They are already starting to keep online secrets from their parents and don't share their passwords as readily. Some try and avoid their parents' supervision and use chat lingo to avoid their parents understanding their communication. They pretend a great deal at this age. Pretending to be older, more popular, richer, a better athlete, etc. is commonplace. They are experimenting all the time.

As they are starting to grow up, they may be entitled to more privacy (when discussing young crushes and other private information). But balancing their privacy with supervision is something parents need to learn to do. They may want more privacy and freedom than they should have at this age. You'll have to decide that for yourself, based on your preteen. The more balanced their activities are (offline friends, sports, after school activities and hobbies) the safer they usually are online. But, trust needs to be earned on both sides.

School assignments may require more access to websites than the younger parental control settings would allow. And the more restrictive kid-sized search engines may not give them access to the sites they need, either. And, when they are upset and online, they are more likely to act out. So teaching them to Take5! and ThinkB4UClick are important lessons at this age. (You can learn more in the "Ms. Parry's Guide to Netiquette" chapter and the chapter on cyberbullying.)

They may start using peer-to-peer software to illegally download music at this age. Keep an eye out for their use of file-sharing software (like Kazaa or Limewire), since there is no good reason a child of this age should be using it at all. Consider buying them a music service subscription service, like Yahoo's or

Napster's, or giving them an account at iTunes.

- Raise the bar on parental controls and filtering programs to allow them to access websites they need for school, or use a parental control software that allows you to unblock sites from a remote location, by e-mail override.
- Start using full-sized search engines with filters applied (check their advanced settings) or use a toolbar (Google's comes preset with a medium filter).
- Cyberbullying is a serious problem at this age, watch for the signs…
- Teach them about personal information and predators. Without going into details, they are concerned about people showing up at their house. Make sure they remember this when online or on text-messaging devices.
- Watch for "away messages" for their IM programs. Kids often post their cell phone numbers there.
- Websites and profiles they build should be reviewed carefully, as should screen names.
- Make sure that you control the family account password and have their passwords too. Expect some push-back.
- Give them privacy as long as it is with people you trust.
- Block all but pre-approved senders. (Expect push-back here too.)
- Make sure they can't share pictures online, or set up profiles, blogs or webcams without your okay.
- Interactive games should still be limited to Toontown.com and other kid-approved sites. They are still too young for X-Box Live, without direct parental supervision or parental controls. (X-Box won one of our safe gaming awards for its parental controls.)
- Watch early media piracy, teach them not to steal online or offline.
- Google their name, screen names, address, and telephone numbers at least once a week and create alerts to warn you of any new postings. Many kids post nasty things about others at this age. (Read about how to Google someone in Step Three, Implementing and Enforcing Your Choices.)
- Change their passwords often and make sure that they aren't using a provocative screen name.
- Search regularly on your computer for images (of porn or of your kids), and any music, movie or media files you don't know about.
- Spyware is a serious problem at this age, since they often access game sites riddled with spyware and malicious code.
- Lock your private files with a password they don't know.
- Get them started in online safety education, check out wiredkids.org or internetsuperheroes.org. Check out starting a tweenangel chapter at your local school. (For more information visit teenangels.org.)
- Watch cell phone gaming, porn and spending capabilities, and think about limiting their cell phone usage in a way that shuts it down when they exceed it, instead of just charging you extra. (Check into filtering products for cell phone Internet access.)

Between 13and 15 years of age:
The risk of Internet sexual predators and Internet sexual exploitation is highest at this age. They have the freedom to meet the Internet "friends" in the mall or in other public places and their being away from home (at the movies, etc.) isn't questioned as it would have been a few years ago. Their hormones are raging, and they are more sexually inquisitive at this age too. Our studies have shown that a surprisingly high percentage of girls at this age admit to engaging in cybersex (having graphic sexual communications online, typically with strangers they encounter.) In one of our studies 60% of the girls we polled between 13 and 16 years of age admitted to engaging in cybersex.

It gets tricky, as they need more privacy at this age than ever before, yet also need more supervision and guidance. Respect their privacy more and talk with them about their online experiences. If you use monitoring software, use it for emergencies - never accessing the reports until something goes wrong and you need to. Consider them the security video camera in the corner of the bank. No one reviews the tapes until there is a bank robbery. And then they are invaluable.

Their mobile devices are their lifeline at this point in their young lives. Text-messaging is crucial to their social life and if they are offline for a few hours, everything falls apart. ☺ Maintaining balance is harder too. And no one website or collection of websites holds their loyalty. In fact, they surf much less than ever before, spending their online time posting on social networking profiles, building their own websites, setting up webcams and instant and text-messaging their friends. Perhaps social networking websites and

blog sites are more of a risk for teens in this age range for than for anyone else. And, since they have a huge influence on money spent offline and have lots of their own money to spend (from holiday gifts, babysitting and other jobs), they are targeted by marketing schemes and ads of all kinds. Unfortunately, everything they had practiced until now on safe and secure technology use is often thrown out the window in their quest for new thrills and to be treated like young adults. They will sometimes at this age engage in sexual discussions and intentionally meet adults offline for sexual purposes. At least one study reflected that 1 in 4 girls and 1 in 7 boys in this age range were meeting strangers offline.

They are also listening, accessing and downloading music online and sometimes accessing movies and software though peer-to-peer websites, illegally. (Although most of the movie, software and gaming piracy occurs when they are in university, not middle or high school.)

Online gambling, eating disorders, bomb-building and other more dangerous websites hold their greatest appeal to kids in this age group. They experiment often and push the envelope, challenging your rules. Even if you remain consistent in your rules and use of parental control technologies, they are more likely to use handheld devices and their friend's Internet access to circumvent them.

Cyberbullying becomes cyber-sexual-harassment and more mean-spirited. Hacking, malicious code attacks and cyber-stalking become more common place when their tech skills improve and their access to higher powered technologies increase. Posing and password theft is a serious problem too. Sadly, the typical culprit is a close friend or former friend.

They are buying things online at this point, often bidding for things they collect on eBay and other auction websites. They may have their own e-commerce accounts and credit cards they are using online. That means that ID theft and financial credential theft are more prevalent at this age too. And scammers and con artists often target young teens, knowing that they may be less careful than they should be and may be conned into giving away your banking information.

- Filter sites that are inappropriate for young teens, instead of blocking all but approved sites. Some bad ones will get through, though. So talk about it beforehand.
- Give them more leeway on people they can accept IMs or e-mails from. But check and account for everyone, in real life, on their buddy list. No friends of friends.
- Make sure you filter or block image searches (a way around many filters).
- Block peer-to-peer technologies and get your kids an account with iTunes or another legal music download site, or even better, one of the new subscription services, like Yahoo!.
- Teach them to guard their passwords. Password theft is a serious problem at this age.
- Teach them not to pirate or illegally download or share software, games, music or motion pictures.
- Have them Google themselves often, screen names, telephone and cell numbers, addresses, full names, nicknames, etc. (all in quotation marks to search the whole phrase).
- Try and limit their use of chatrooms to monitored chatrooms or themed chatrooms on safe topics.
- Limit their online use (including text-messaging) to under 1-1/2 hours a day (aside from a special school project).
- Keep them out of social network or online dating sites (like xanga.com, friendster.com or match.com).
- Talk to them about not meeting strangers offline, and agree to go with them or teach them large group safe meeting tips (see "Step 3- Implementing and Enforcing Your Choices")
- Get girls (and boys) a copy of Katie Tarbox's book "A Girl's Life Online" (formerly known as "Katie.com") to read. (Katie founded Katiesplace.org, a website for young victims of Internet sexual exploitation and their families and friends.)
- Try to keep the computer in a central location, if it has Internet access, and watch new interactive devices, like cell phones, text messaging devices and interactive gaming devices, like X-Box Live. Use parental controls if they come with them. (X-Box Live got an award from us for their safety devices and parental controls.) But note that even with parental controls, these games are risky for young teens when they chat with strangers.
- Consider setting up a teenangels.org chapter, or starting an online safety club at their school. (Visit Marvel comic-themed Internetsuperheroes.org for available free materials.)
- Pick your battles! Not all risks are created equal online. Let things like their use of inappropriate and even sometimes lewd language go, understanding it's how kids talk online, and focus on their sharing too much personal information or meeting strangers.

- Talk to them about protecting their friends' privacy too.

For 16 years of age and over:
All bets are off. If they have earned your trust, give it to them. If not, unplug the computer and take away their cell phones and interactive gaming devices. And pray often and hard. ☺ If you haven't taught them what they need to know by now, we're all in trouble.

- Focus on teaching them to be responsible cybercitizens and to use the filter between their ears.
- Emphasize the risks of sharing personal information and meeting strangers offline.
- Make sure they Google themselves often and report what they find. Have them set an alert on themselves as well.
- Teach them to use anti-virus programs, not believe everything they read online and to respect others. Check for adware or spyware often, use a firewall and teach them to come to you if anything goes wrong online. (Maybe they will.)
- And get their help in keeping their younger brothers and sisters safe online.
- Remind them that you're still around if they need your help.
- Pick your battles! Not all risks are created equal online. Let things like their use of inappropriate and even sometimes lewd language go, understanding it's how kids talk online, and focus on their sharing too much personal information or meeting strangers.

Appendix 4: Parenting Online - WiredSafety.org's booklet for parents - printable online

Parenting Online

What do we do when our eight-year-old knows more than we do about cyberspace? How do we guide our children safely through this new world? How do we set the rules when we don't even understand the risks? The childproof locks, seatbelts and helmets we use to help keep them safe in everyday life won't protect them in cyberspace. There we need new and different gadgets and safety tips.

Welcome to the new world of parenting online! It's your newest challenge. But don't worry...it's not as hard as you think and it's well worth the effort.

Parenthood is never easy and the ground rules are always changing. We go from playing the role of confidante, to co-conspirator, to police chief, to teacher, to playmate and back...all in the same day. We barely have the chance to catch our breath!

The things we do to make sure our children stay safe are constantly changing too. When they crawl, we learn how to keep things off the floor. Then, they pull themselves upright, we have to keep them safe from the new dangers at eye level. Training wheels have to be removed, and we have to watch while they pedal away (generally into the nearest tree). We watch their sugar intake, make sure they take their vitamins and keep small items out of their mouths.

That's our job, as parents. So the tried and true warnings, passed down from generation to generation, are repeated... "don't talk to strangers...," "come straight home from school...," "don't provoke fights...," "don't tell anyone personal information about yourself..." and "we need to meet your friends..." This is familiar territory after all. We know the dangers our kids face in the street or at the mall or in the school yard, because we faced them.

As in any large community, there are dangers our children encounter in cyberspace, too. But, since our children know more than we do about cyberspace, we worry about how we can teach them to avoid those dangers. Don't panic... those dangers can be managed using the same old warnings we've always used.

We just need to translate them into cyberspace terms...

And there are wonders around every cyber-corner too...

The Internet is the largest collection of information in the world, always available without a charge and delivered to your home computer. Every question you might have can be answered online. When your child asks you how deep the ocean is or why the sky is blue, you can "ask the Internet," together.

You and your children can communicate with others too, worldwide and in every language, with the click of your mouse. Their artwork can be displayed, their news reporting published and their poems posted on the largest "refrigerator door" in the universe, where 700 million people can appreciate them.

You can research your family tree and build a family Web site. And, best of all...the most complicated homework assignment can be researched online (even last-minute on the Sunday night before it's due).

You can search online for just about anything and any information you want. The easiest way to do that is by using search engines. You can type your search into one of the search engines and often will find what you are seeking. Just as often, though, you will find sites that are trying to get your or your children's attention. Pornographers are the most frequent abusers of search engines, registering and coding their sites to trick people into visiting them, thinking they are Disney, Pokemon or even the White House.

Most of the search engines now have filtering options. By selecting one of these options, most inappropriate content is filtered out and the search results are typically kid-friendly. Two commercial search engines were designed just for kids, though, and are wonderful places to begin your child's search online. Yahooligans!, Yahoo! kid-sized search engine hand-selects the sites, making sure nothing slips through. It is best for younger children, ten and under. Ask Jeeves for Kids is Ask Jeeves kid-sized search engine. Although not as scrubbed clean as Yahooligans! hand-selected sites, it contains many more sites which make it perfect for slightly older children. I recommend it for children ten and older.

In addition, most full-size search engines have a filtered option you can select. But remember that even if you use a search engine filter, if the kids search for images, the can find things you wish they hadn't. That's when using a filtering product that can block images too might come in handy.

In addition to kid-sized search engines, there are many wonderful family-friendly site lists. WiredKids has one of its own, where the sites are selected and reviewed by our specially-trained volunteers. You can even recommend your favorite sites to be added.

There are some entertaining sites that teach children online safety, as well. Although we prefer our WiredKids.org, StopCyberbullying.org and InternetSuperHeroes.org the best, (she says modestly...) another very special one we want to point out. Disney's Surfswellisland.com teaches online safety Disney-style. Mickey Mouse, Donald Duck, Minnie Mouse and Goofy all find themselves involved in tropical island cyber-challenges relating to viruses, privacy, netiquette (cyber-etiquette) and responsible surfing. Lesson plans, online safety worksheets and other wonderful resources are all available without charge at the site.

Looking for homework help? Check out Discovery.com, Nationalgeographic.org, PBSkids.org and The National Gallery of Art kids page www.nga.gov/kids/kids.htm**.** And ask your school librarian or the librarian at your public library for sites they recommend. Librarians and library media specialists are the guides to valuable and safe online resources for children. And if you need something you can't find, send me an email at "Ask Parry," (askparry@wiredsafety.org) my Internet-syndicated online safety column. Drop by WiredKids.org or WiredSafety.org to find out how to submit a question.

CyberSense
...translating common sense for cyberspace

- **Don't talk to or accept anything from strangers.** That's the first one we learn while growing up, and the first one we teach our children. The problem in cyberspace though is teaching "stranger danger." Online, it's hard to spot the strangers.

  The people they chat with enter your home using your computer. Our kids feel safe with us seated nearby. Their "stranger" alerts aren't functioning in this setting. Unless they know them in real life, the person is a stranger no matter how long they have chatted online. Period. You need to remind them that these people are strangers, and that all of the standard stranger rules apply.

  You also must teach them that anyone can masquerade as anyone else online. The "12-year-old" girl they have been talking to may prove to be forty-five year old man. It's easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace.

- **Come straight home after school.** Parents over the generations have always known that children can get into trouble when they wander around after school. Wandering aimlessly online isn't any different. Parents need to know their children are safe, and doing something productive, like homework. Allowing your children to spend unlimited time online, surfing aimlessly, is asking for trouble.

  Make sure there's a reason they're online. If they are just surfing randomly, set a time limit. You want them to come home after they're done, to human interaction and family activities (and homework).

- **Don't provoke fights.** Trying to provoke someone in cyberspace is called "flaming." It often violates the "terms of service" of your online service provider and will certainly get a reaction from other people online.

  Flaming matches can be heated, long and extended battles, moving from a chat room or discussion group to e-mail quickly. If your child feels that someone is flaming them, they should tell you and the sysop (system operator, pronounced sis-op) or moderator in charge right away and get offline or surf another area. They shouldn't try to defend themselves or get involved in retaliation. It's a battle they can never win.

- **Don’t take candy from strangers.** While we don’t take candy form people online, we do often accept attachments. And just like the offline candy that might be laced with drugs or poisons, a seemingly innocent attachment can destroy your computer files, pose as you and destroy your friends or spy on you without you even knowing it. Use a good anti-virus, update it often and try one of the new spyware blockers. You can get a list of the ones we recommend at WiredSafety.org. Practice safe computing!

- **Don't tell people personal things about yourself.** You never really know who you're talking to online. And even if you think you know who you are talking to, there could be strangers lurking and reading your posts without letting you know that they are there. Don't let your children put personal information on profiles. It's like writing your personal diary on a billboard.

  With children especially, sharing personal information puts them at risk. Make sure your children understand what you consider personal information, and agree to keep it confidential online and everywhere else. Also teach them not to give away information at Web sites, in order to register or enter a contest, unless they ask your permission first. And, before you give your permission, make sure you have read the web site's privacy policy, and that they have agreed to treat your personal information, and your child's, responsibly.

- **We need to get to know your friends.** Get to know their online friends, just as you would get to know their friends in everyday life. Talk to your children about where they go online, and who they talk to.

- **R-E-S-P-E-C-T.** We all know the golden rule. We have a special one for cyberspace. Don’t do anything online you wouldn’t do offline. If you teach your child to respect others online and to follow the rules of netiquette they are less likely to be cyberbullied, become involved in online harassment or be hacked online. You can learn more about the ways to combat cyberbullying at our new website, StopCyberbullying.org or at WiredSafety.org’s cyberstalking and harassment section. Remember that it is just as likely that your child is a

cyberbully (sometimes by accident) as a victim of one. Let them know they can trust you not to make matters worse. You have to be the one they come to when bad things happen. Be worthy of that trust.

Remember that the new handheld and interactive gaming devices you buy have real risks to. Your children can send and receive text-messages from anyone on their cell phones or text-messaging devices and interactive games allow them to chat, on Internet phone, to anyone who wants to talk with them. The new Bluetooth devices let your child receive messages form anyone in a 300 foot range, and could be a problem if they play the new Bluetooth handheld games in a mall. Think about the features you are buying when you buy new devices for your children. Check into privacy and security settings. Our Teenangels (teenangels.org) are working on new guides for parents and other teens on what to look for and think about before you buy a new interactive device. Look for them at your local retailer or on the WiredSafety.org and Teenangels.org websites.

Don't just set up the computer in the corner of their bedroom, and leave them to surf alone. Take a look at their computer monitor every once in awhile, it keeps them honest. Sit at their side while they compute when you can. It will help you set rules that make sense for your child. It also gives you an unexpected benefit...you'll get a personal computing lesson from the most affordable computer expert you know!

And it's worth the effort. When our children surf the Internet, they are learning skills that they will need for their future. They become explorers in cyberspace, where they explore ideas and discover new information.

Also, because there is no race, gender or disability online, the Internet is the one place where our children can be judged by the quality of their ideas, rather than their physical attributes.

What Tech Tools Are Out There?

Blocking, filtering and monitoring...when you need a little help

There are many tools available to help parents control and monitor where their children surf online. Some even help regulate how much time a child spends playing computer games, or prevent their accessing the Internet during certain preset times.

I've listed the type of protections that are available. But, most of the popular brands now offer all of these features, so you don't have to choose. Recently, given parents' concerns about strangers communicating with their children online, monitoring software has gained in popularity. Although it might have its place in protecting a troubled child, it feels more like "spyware" than child protection. But it's ultimately your choice as a parent. The newest trend is to use products supplied by your ISP called parental controls. AOL's parental controls were the first of these to be developed and used. MSN 8.0 launched the first set of parental controls for MSN. To read more about the various products and services we have reviewed, visit WiredKids.org and WiredSafety.org.

Blocking Software

Blocking software is software that uses a "bad site" list. It blocks access to sites on that list. They may also have a "good site" list, which prevents your child from accessing any site not on that list. Some of the software companies allow you to customize the lists, by adding or removing sites from the lists. I recommend you only consider software that allows you to customize the list, and lets you know which sites are on the lists.

Filtering

Filtering software uses certain keywords to block sites or sections of sites on-the-fly. Since there is no way any product can keep up with all the sites online, this can help block all the sites which haven't yet been reviewed. The software blocks sites containing these keywords, alone or in context with other keywords.

Some companies allow you to select certain types of sites to block, such as those relating to sex, drugs or hate. This feature engages special lists of keywords that match that category. As with the "bad site" lists, the lists of keywords used by the filtering software should be customizable by the parent, and every parent should be able to see which terms are filtered.

Outgoing Filtering

No...this doesn't mean your software had a sparkling personality :-) (that's cyberspace talk for "grin" and means you're supposed to smile at my brilliant humor, and if you want to learn more about this stuff...you need to read my Ms. Parry's Guide to Correct Online Behavior). It means that your child won't be able to share certain personal information with others online. Information such as your child's name, address or telephone number can be programmed into the software, and every time they try to send it to someone online, it merely shows up as "XXXs." Even with kids who know and follow your rules, this is a terrific feature, since sometimes, even the most well-intentioned kids forget the rules.

Monitoring and Tracking

Some software allows parents to track where their children go online, how much time they spend online, how much time they spend on the computer (such as when they are playing games) and even allows parents to control what times of day their children can use the computer. This is particularly helpful when both parents are working outside of the home, or with working single-parents, who want to make sure their children aren't spending all of their time on the computer. Many parents who don't like the thought of filtering or blocking, especially with older children and teens, find monitoring and tracking satisfy their safety concerns. They can know, for sure, whether their children are following their rules.

We particularly recommend using a monitoring software and then forgetting it's installed. Think of it as the security video camera in the corner of the bank. No one views the tapes until the bank is robbed. If something bad happens, you can play back the monitoring log and see exactly what occurred, and who said what, and in dire situations, where your child went to meet an adult offline. We particularly like Spectorsoft.com, because their products can monitor all instant messaging platforms, which is key to keeping your children safe online.

Parents have to remember, though, that these tools are not cyber-babysitters. They are just another safety tool, like a seat belt or child safety caps. They are not a substitute for good parenting. You have to teach your children to be aware and careful in cyberspace. Even if you use every technology protection available, unless your children know what to expect and how to react when they run into something undesirable online, they are at risk. Arming them well means teaching them well.

Your Online Safety "Cheatsheet"

Some Basic Rules for You to Remember as a Parent . . .

- Make sure your child doesn't spend all of her time on the computer. People, not computers, should be their best friends and companions.
- Keep the computer in a family room, kitchen or living room, not in your child's bedroom. Remember that this tip isn't very helpful when your children have handheld and mobile Internet and text-messaging devices. You can't make them keep their cell phones in a central location. So make sure that the "filter between their ears" is working at all times.
- Learn enough about computers so you can enjoy them together with your kids.
- Teach them never to meet an online friend offline unless you are with them.
- Watch your children when they're online and see where they go.
- Make sure that your children feel comfortable coming to you with questions and don't over react if things go wrong.
- Keep kids out of chat rooms or IRC unless they are monitored.
- Encourage discussions between you and your child about what they enjoy online.
- Discuss these rules, get your children to agree to adhere to them, and post them near the computer as a reminder.
- Find out what e-mail and instant messaging accounts they have and (while agreeing not to spy on them) ask them for their passwords for those accounts.
- "Google" your children (and yourself) often and set alerts for your child's contact information. The alerts will e-mail you when any of the searched terms are spotted online. It's an early warning system for cyberbullying posts, and can help you spot ways in which your child's personal information may be exposed to strangers online. To learn how to "Google" them, visit InternetSuperHeroes.org.
- Teach them what information they can share with others online and what they can't (like telephone numbers, address, their full name, cell numbers and school).
- Check your children's profiles, blogs and any social-networking posts. Social-networking websites include myspace.com, facebook.com and xanga.com. (We work closely with MySpace and Facebook to help keep their users safer.) Social networks, generally, shouldn't be used by preteens and should be only carefully used by teens. Yfly.com is a new teen-only social network that is designed from top to bottom to keep teens safer and teach them about more responsible behaviors.
- For those of you with preteens and young teens, read the Safer Social Networking guide at WiredSafety.org.
- Get to know their "online friends" just as you get to know all of their other friends.
- Warn them that people may not be what they seem to be and that people they chat with are not their friends, they are just people they chat with.
- If they insist on meeting their online friend in real life, consider going with them. When they think they have found their soul mate, it is unlikely that your telling them "no" will make a difference. Offering to go with them keeps them safe.
- Look into the new safer cell phones and cell phone features that give you greater control over what your children can access from their phone and how can contact them.

PARENTING ONLINE
MY AGREEMENT ABOUT USING THE INTERNET

Once you understand enough about cyberspace and how your children surf the Internet, you can set your own rules. These are the basic rules, even though you may want to add some of your own.

Some kids like setting the rules out clearly in an agreement. Here's one you can use, and post near your computer to help them remember how to surf safely. (Note that while the tips may work for teens, the contract is designed for preteens and younger.)

I want to use our computer and the Internet. I know that there are certain rules about what I should do online. I agree to follow these rules and my parents agree to help me follow these rules:

1. I will not give my name, address, telephone number, school, or my parents' names, address, or telephone number, to anyone I meet online.
2. I understand that some people online pretend to be someone else. Sometimes they pretend to be kids, when they're really grown ups. I will tell my parents about people I meet online. I will also tell my parents before I answer any e-mails I get from or send e-mails to new people I meet online.
3. I will not buy or order anything online without asking my parents or give out any credit card information.
4. I will not fill out any form online that asks me for any information about myself or my family without asking my parents first.
5. I will not get into arguments or fights online. If someone tries to start an argument or fight with me, I won't answer him or her and will tell my parents.
6. If I see something I do not like or that I know my parents don't want me to see, I will click on the "back" button or log off.
7. If I see people doing things or saying things to other kids online I know they're not supposed to do or say, I'll tell my parents.
8. I won't keep online secrets from my parents.
9. If someone sends me any pictures or any e-mails using bad language, I will tell my parents.
10. If someone asks me to do something I am not supposed to do, I will tell my parents.
11. I will not call anyone I met online, in person, unless my parents say it's okay.
12. I will never meet in person anyone I met online, unless my parents say it's okay.
13. I will never send anything to anyone I met online, unless my parents say it's okay.
14. If anyone I met online sends me anything, I will tell my parents.
15. I will not use something I found online and pretend it's mine.
16. I won't say bad things about people online, and I will practice good netiquette.
17. I won't use bad language online.
18. I know that my parents want to make sure I'm safe online, and I will listen to them when they ask me not to do something.
19. I will help teach my parents more about computers and the Internet.
20. I will practice safe computing, and check for viruses whenever I borrow a disk from someone or download something from the Internet.
21. I won’t post my cell number on my away message, and will check with someone before posting something personal about me on my blog or on a networking site.
22. I will Stop, Block and Tell! If I am harassed online or cyberbullied.
23. I will Take 5! before reacting to something that upsets me or makes me angry online.
24. I will practice responsible ”thinkB4Uclick” rules. (I know I can find out more about these things at InterentSuperHeroes.org and StopCyberbullying.org.)
25. I will learn how to be a good cybercitizen and control the technology, instead of being controlled by it.

_____

I promise to follow these rules. (signed by the child)

_____

I promise to help my child follow these rules and not to over react if my child tells me about bad things in cyberspace (signed by parent).

From Parry:

I am asked questions about kids online safety at least a hundred times a day. Is the Internet a dangerous place? Are there predators out there looking to set up a meeting with my child? How can we find good and reliable content online? How can I supervise my child's surfing when I can't even turn on the computer?

These any other question like these fill my inbox daily. (If you have a question of your own, visit WiredKids.org or WiredSafety.org and click on "Ask Parry." Here is the one simple answer:

The single greatest risk our children face in connection with the Internet is being denied access. We have solutions for every other risk.

That bears repeating, over and over, especially when we hear about Internet sexual predators, hate, sex and violence online. But our children need the Internet for their education, careers and their future.

Happily, most of the risks are easily confined. In each and every case when children encounter Internet sexual predators offline, they go willing to the meeting. They may think the person is a cute fourteen year old girl or boy, but they know they are meeting someone they don't know in real life. That means we can prevent 100% of these crimes. Merely teach our children not to meet Internet strangers offline. If they are set on meeting that person anyway, go with them. That way, if the person turns out to be a cute fourteen year old, you are the hero. And if they aren't, you're an even *bigger* hero.

Our WiredKids, WiredTeens and Teenangels programs, in addition to being fun and educational sites, are also volunteer programs where children and teens are taught online safety and privacy and responsible surfing. They then use these skills to help other children and teens learn to surf safely, as well. Talk to your children about what they do online (and offline also), and let them know you are there to help if things go wrong. You will note that in our safe surfing agreement parents have to promise only one thing...not to overreact if their children come to them for help. Earn their trust, and be worthy of it. Register your children at WiredKids.org, our children's online safety site, and we will make sure they learn what they need to know about enjoying the Internet safely and privately. It's not about technology at all...it's about communication and good parenting.

Remember, we're all in this together!

Parry
Parry Aftab, Esq.
Executive Director
WiredSafety.org and its family of sites and programs, including Teenangels.org, WiredKids.org and CyberLawEnforcement.org

WiredSafety is a 501c-3 non-profit organizations formed under the laws of the State of New York. (Its legal name is "Wired Kids, Inc.") This publication is copyrighted to Parry Aftab, Esq. All rights reserved. For permission to duplicate this publication, contact parry@aftab.com.

Appendix 5: More about WiredSafety.org

WiredSafety, is a 501(c) (3) charity and the largest and oldest online safety, education, and help group in the world. Begun as a group of volunteers rating websites in 1995, it now provides one-to-one help, up-to-date information, and education to cyberspace users of all ages on anything that can go wrong online. These services are offered through a world-wide system of volunteers, who make up their various teams and divisions, and administer their specialized sites and programs. With the exception of our Teenangels, outreach and speaking programs, all work and help is provided online and without charge. All within WiredSafety.org are unpaid volunteers, including its founder and Executive Director, cyberlawyer Parry Aftab.

WiredSafety's work falls into four major areas:

- **Help** for online victims of cybercrime and harassment
- **Assistance** for law enforcement worldwide on preventing and investigating cybercrimes
- **Education** for children, parents, communities, law enforcement, and educators
- **Information and Awareness** on all aspects of online safety, privacy, responsible use and security

WiredSafety's audience and the key stakeholders include:

- Parents, grandparents and caregivers;
- Kids, preteens, teens and college students;
- Members of the Internet and interactive technology industries;
- Law enforcement, the judicial community and regulatory agencies; and
- Schools and educational institutions

Together with their wiredcops.org program, specially-trained volunteers assist with cases of child pornography, child molesters, and cyberstalkers. WiredSafety also offers a wide variety of educational and help services to the Internet community at large. Companies such as Disney, Yahoo!, Oracle, MySpace, Facebook, Microsoft and AOL turn to Parry Aftab and WiredSafety.org for guidance and help. Other volunteers find and review family-friendly Web sites, filtering software products, and Internet services. Some of the outreach team volunteers run programs, summit and also speak at local community groups and schools around the world teaching Internet safety, privacy and responsible use.

And its work is not limited to the Internet alone. WiredSafety focuses on all aspects of interactive technology use and abuse. Its expertise includes cell phone safety and security, interactive gaming, social networking (mobile and online) and text-messaging products, as well as any new interactive technologies as they are developed. Its long years of working with Internet users and handling cybercrimes and abuse have created a flexible and knowledgeable volunteer force. If you can view content, communicate with others or spend money or buy things using the technology, WiredSafety can help.

Its help also involves one-to-one assistance for cases of cyberabuse. WiredSafety's cyberhelp line gives netizens access to free help when they need it online. Its special team of help volunteers are assigned to cases and work one-to-one online to help resolve your problems and get you help when you need it. WiredSafety handles more cases of cyberstalking than any other organization in the work, helping

thousands each month through its site and reportline. Cyberbullying cases can be reported to the reportline as well.

The new focus on cyber-wellness and cyberethics fits perfectly within WiredSafety's mission and expertise. As we raise a new generation of cybercitizens, they need to understand the norms and rules of operating online. They must also recognize that they must be held accountable for what they do in cyberspace and that what they post online has ramifications beyond the momentary click. Marvel joined forces with WiredSafety to provide superhero assistance in educating our children and families on safer online practices. The first Internet safety comic, Internet Super Heroes meet the Internet Villains, teaches how Internet predators can infiltrate anyone's computer and wreck havoc on their lives by stealing their identity and posing as them online. Published under our exclusive license with Marvel, and sponsored by Microsoft, this comic will help teach the 250,000 readers how to be smart and safer online.

WiredSafety is proud of its reputation as the one-stop-shop for all cyberspace safety, privacy, security, and help needs. It is even prouder of the fact that all this can be accomplished without large government funding or money wasted on administration costs. Its volunteer workforce has been estimated at providing more than $3 million in unpaid services every year. It has operated since 1995 with a total funded budget of under $150,000 a year.

WiredSafety is headed by Parry Aftab (also a volunteer), a mom, international cyberspace privacy and security lawyer and children's advocate. Parry is the author of the first book written for parents about Internet safety - The Parents Guide to the Internet (considered the bible of online safety and published in 1997) as well as The Parent's Guide to Protecting Your Children in Cyberspace (McGraw-Hill, 2000), which has been adapted and translated around the world. Her most recent books have been especially written and adapted for and published in England, China, Spain and Singapore. Her new book, Internet Safety 1-2-3 will be released this year in the United States. It was released in December 2005 in Spain.

WiredSafety volunteers range in age from 18 to 80. WiredKids range from seven to twelve, and the Teenangels from 13 to 18. These programs run in conjunction with WiredKids.org, one of WiredSafety's division. WiredSafety backgrounds include everything from TV personalities, teachers, stay-at-home moms, retired persons, law enforcement officers, and students to PhD's and writers.

For law enforcement officers, WiredSafety provides information and resources to help educate and guide officers on Internet safety issues and crime prevention and reporting of cybercrimes. It also has a special website just for law enforcement officers, Cyberlawenforcement.org and WiredCops.org.

It is also the only organization that uses expert trained teens and preteens to help develop safer technologies, by advising members of the Internet industry and governmental agencies around the world. These expert Teenangels (and now their younger version, Tweenangels from 9 - 12 years of age) deliver the message of safe, private, and responsible technology use to their peers. These youth-based programs were formed in 1999 to provide special perspectives and insight into how young people are using the new technologies and how to better prepare them to handle the risks they encounter. Teenangels have been recognized and honored by Congress, John Walsh and recently, Teen People Magazine, among others. Recently, at the request of leading law enforcement agencies, WiredSafety has begun using its young volunteers to provide information that will assist undercover law enforcement officers in being more believable when posing as young teens.

Originally formed to provide help and protection for Internet users of all ages, Wiredsafety's work has become more and more focused on children, tweens, and teens in recent years. WiredSafety is dedicated to protecting children in cyberspace from cybercrimes and abuse, including from each other. This involves protecting them from cyberbullying, hacking, sexual harassment and identity (ID) theft. It also includes protecting children everywhere from Internet-related sexual exploitation, including assisting law enforcement in the investigation and prevention of trafficking of children, child pornography, and organized child molester groups.

WiredSafety's experience is particularly effective in assisting law enforcement agencies in improving their undercover skills.