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)

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY, SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING AND TERRORISM ASSESSMENT

November 6, 2007, 2:00 pm

CANNON HOUSE OFFICE BUILDING, ROOM 311

"Using the Web as a Weapon: The Internet as a Tool for Violent Radicalization and Homegrown Terrorism"

Parry Aftab, Esq.
"The Kids Internet Lawyer" and
Executive Director, WiredSafety.org
Email:parry@aftab.com
www.aftab.com
201-463-8663

SUMMARY

Our children and young adults are online. They do their school work, entertain themselves, communicate with each other and us, research things, shop for things, learn and work, 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 guaranteed that they are hurt. All other risks are avoidable through a combination of awareness, supervision, trained law enforcement investigators and the adoption of best practices and risk management by educational institutions and the Internet industry itself.

This testimony will focus on the darker side of the Internet, especially Web 2.0 technologies and social networks. I respectfully caution this Subcommittee not to consider throwing the Internet out with the cyberrisks bathwater. As I have said over and over for the last twelve years, all risks can be contained and managed with the right combination of analysis of the risks, measurement of their impact and evaluation of use of the technologies.

This requires that we engage the Internet industry itself and advise them in ways to build safer technologies and adopt best practices designed to make all their users, not just children, safer. It also requires that we engage law enforcement agencies in discussions with the industry and cybercrime prevention non-profits, such as WiredSafety.org, in forming and deploying solutions.

OPENING STATEMENT

Good afternoon, Chairwoman Harman and other esteemed members of this Sub-Committee. I would like to thank this Sub-Committee for inviting me to testify today and share my expertise on young people online. I will focus my testimony today on how radicalization and homegrown terrorism groups can use the Internet to reach at-risk youth and recruit followers from the ranks of teens and young adults. I will also suggest ways we can address these risks, in particular ways Congress can help address them.

My name is Parry Aftab, and I am an Internet privacy and security lawyer and founded and run the world's largest cybersafety and help group, WiredSafety.org. I have worked in the field of cyber-risk management and cybercrime prevention since the Web was launched in 1993. I was appointed by UNESCO to head up its online child protection initiative in the United States and formed and run a charity that contains more than 12,000 volunteers from around the world. WiredSafety.org's special group of trained volunteers offer one-to-one help to victims of cyberabuse and assist law enforcement, parents, schools and communities manage online risks and prevent cybercrimes. We see all risks, on all digital technologies for all ages of users on a daily basis.

My testimony will pull from my personal experience, that of the charity, our work with law enforcement and regulatory agencies and extensive polls of young people. It will focus on how Web 2.0 technologies and networks are allowing radical groups access to young users and the ability to spot more vulnerable and at risk youth for recruitment.

Identifying the Problem

Most of the teens and young adults in the United States are using social networks and other Web 2.0 technologies. These include MySpace, Facebook, Bebo, Xanga, Google's Blogspot and its new social network - Orkut, BlackPlanet and MiGente and Hi5, as well as X-Box 360, PSP2, DS, World of Warcraft, Runescape and other interactive gaming sites and technologies. It has fast become their favorite online activity, after instant messaging.

While accurate statistics of minors' use of social networks do not exist (with many lying about their age or identities), statistics as to social network traffic and usage of all registered users are regularly tracked.. According to HitWise, a leading industry reporter, MySpace traffic accounted for almost 5% of all US cybertraffic, with Facebook accounting for almost 1% of all cybertraffic during the week of October 13, 2007. And all social networks in the US combined accounted for almost 7% of all online traffic during the same time, up about 20% from last year.

They use it to communicate with others, either existing friends in the real world or new ones in the virtual world. They use it to share ideas and showcase their talents and interests. They use it to persuade others to take action on important issues. They use it to network with others and recruit people to their cause or candidate. They use it to find other like-minded people or people who are different from them. They seek out what others are doing in big cities, affluent communities, other countries or next door. They look for love and romance and excitement. They search for long-lost friends, kids they went to camp with and former classmates. They post pictures and video, using their computers, cellphones and iPods. They share secrets and vulnerabilities, looking for someone to listen. They exploit the secrets and vulnerabilities of others. They lie and steal, learn and teach. They promote content, people and causes by tagging and commenting and rating profiles and multi-media content. And they pose as someone else, or something else to try on new personas or lifesyles. They influence and are influenced on these networks. They do it for the same reasons young people have always done things. They do it for good, for bad, for fun and for kicks.

While most of the media and governmental investigations have focused on the more traditional risks of pornography, Internet sexual exploitation, cyberbullying and harassment online, other less obvious risks have been largely ignored. These include gangs and hate groups, suicide threats, serious eating disorders, scams and fraud, violence, misinformation and hype, commercial espionage and warfare and, now, radicalization.

For the same reasons other users are setting up profiles and posting videos online, gangs, radical groups and even terrorism groups are harnessing the power of the technology and Web 2.0 to spread their messages, communicate with others and recruit others ot their cause. While that is expected, the surprise comes when we see our young adults and teens being receptive to these tactics.

We are seeing an increase in upper-middle class high school students joining inner-city gangs, seeing them as exciting and fun. Many young people are searching for leadership or a cause to believe in. They are seeking a place where they are accepted and can belong. And never before have they had as many to choose from, all at the click of their mouse, or from their cellphone or gaming device. And because they often do things online that they would never dream of doing in real life, they tend to engage in riskier behavior online and often don't see the line between observing and joining, between curiosity and recruitment. Perceived dangers are seen as exciting. And behind their computers, in the privacy of their home, they give the predators the information they need to push their buttons. They signal their vulnerabilities and what they need and are seeking. They make it easy. Too easy for those who are looking for vulnerabilities. Too easy for radical groups and homegrown terrorism groups.

Young People on Social Networks and Using Web 2.0 Technologies

Social networking, a combination of mini-webpages, blogs and searchable communities, have expanded in recent years, most recently exploding with the growth of MySpace and Facebook. Based upon our polls, we estimate that more than half of the young teens in the US with home Internet access have at least one social networking profile and more than 80% of university students have at least one social networking profile.

Many have 2 to 5 separate profiles on just one site, and most have at least one profile on two or more social networks (not all being used, however). Most users check their profiles and their online networks at least once a week, and in many cases several times a day.

WiredSafety.org and I first began our social networking safety work in 2004, after learning how many young teens and preteens were beginning to use them. Unlike the early AOL profile pages used by teens and preteens in prior years, where the young users could post their contact information and brief statements about their interests, these networks were designed to be interactive. And instead of dry posts of contact and other personal interest information, these networks allowed users to post music, movies, animations, sounds, images and lots of user generated content to their page. When used effectively, this allowed the sharing of ideas and expertise and communication with real life friends. When misused, this allowed the broadcast of vulnerabilities that predators of all types can exploit to target young people. This is when the real dangers arise.

While the media and many others have focused only on the dangers of these networks when used by preteens and teens, it is important that we keep our eye on their good uses and value and why their use has exploded in the three years. We have spent four years studying how and why preteens, teens and young adults use these kinds of sites.

Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life. They raise money for their favorite charity and awareness for new causes.

They can post one message and their 150 best friends can see it right away. Unfortunately, so can those who might not have their best interests at heart. And sadly, in some cases, our teens are acting out, taking risks and exploring involvement with hate groups, gangs and radical groups that promote violence. That's when things can get dangerous, especially for young teens.

Professional Guidance for the Industry and Adoption of Best Practices

Most members of the Web 2.0 industry have set rules for what can and cannot be done on their sites. These are set out in their "terms of service" or "codes of conduct." Most terms of service already forbid radicalization (using language about "promotion of violence"). But forbidding it and spotting it are very different. They typically rely on reports of terms of service violations ("TOS violations") to enforce their rules. They sometime deploy technology and live moderation staff to police their site, independent of the reports.

For example, MySpace set up an image scanning procedure, looking at hundreds of thousands of images each day for sexual content and gang signals and hate images. The majority of their policing, however, occurs when a user reports another for a TOS violation. This is then handled under their existing procedures for that category of violation. They are also, according to reports, scanning their system for registered sex offenders.

This is unusual, though, and limited. Only a small protion of images posted can be scanned. The traffic is too large for existing moderation teams to police effectively. Most networks rely entirely on user reports, since video and other multi-media are difficult to filter and review for contraband content.

Social networks, starting with MySpace in early 2005, have come to me and to WiredSafety for help in managing risks and creating safer experiences for their users. They have sought our help in designing law enforcement

investigator's guides to assist law enforcement when evidence of cybercrimes needs to be obtained from those sites. But their needs are greater than what a cybersafety charity can provide. They need hands-on training, certifications of practices and technologies, enhanced technologies and security practices, guidance on adoption of best practices and ways to avoid cyber-abusive and criminal behaviors. They need to share effective practices with each other in industry leadership councils. They need to anonymously share vulnerabilities they have identified to make the industry itself safer, without losing competitive advantage. They need to train recruit or outsource monitoring and moderation staff, and do it in multiple languages.

Because of our unique experience and over 12 years in this field and because managing risks online in a Web 2.0 environment is like "herding cats" the networks and industry has requested that we deploy our experience in helping create best practice standards and assist in their implementation. In response to this demand, leaders in cybercrime and cyber-risk management and security have joined together to form a center for the Web 2.0 industry that will train the industry, advise the industry and provide tools and expertise to implement best practices, and in certain cases, handle moderation and site policing for these sites. The center will be called "The Wired Trust" and will work with the charity, but be a commercial entity designed to serve the needs of the Web 2.0 industry and those involved in funding advising the industry. Among other risks, The Wired Trust will help manage risks of radical groups and terrorism groups using these networks to recruit and promote their violent missions.

Leaders in the industry are already lining up to join The Wired Trust and find ways to become safer and prevent risks.

It's a start.

Public Policy Solutions, Approaches and Congress's Role

The solution is not blocking or limiting access to Web 2.0 technologies or social networks. Creating a new law prohibiting schools and libraries from allowing underage students and users to access these sites or otherwise locking young people out of these sites seems an obvious approach. While this may appear on its face to be an easy answer, it is neither easy nor the answer.

As more social networks are launched every day, and every ISP, entertainment company and wireless provider is either building a social network or finding a way to integrate social networking and community interactivity into their new and existing sites, it is impossible to block all of them and not other valuable Internet features, sites and content. Instead, schools need to be armed with the tools and risk management expertise to

decide what sites their students can access during school hours from their servers and how to enforce their decisions and policies.

Schools need to decide if their students should have access to *any* non-educational site from school computers, and if so, which ones and for what purpose. They then need to develop a policy communicating this decision and the rules to the students (in language they understand), the teachers, the parents and other caregivers and to their IT team. They need to decide whether they will be using software to help enforce their policy, or merely traditional discipline for violating school policies. That too needs to be communicated to the school community. They also need to create or adopt educational programs teaching their students what information they can and shouldn't be sharing online, the risks of irresponsible Internet use and where to go when things go wrong.

Teaching students about hype and misinformation and about hate and radicalization is crucial as well. If young people learn how they are manipulated by these groups, they are less likely to fall prey to them. At risk youth needs to be supervised, as they are often the earliest targets and most likely to join radical groups that promise them excitement and community combined. Educational institutions can play an important role in teaching their students, parents and other community members about safe, private and responsible Internet and wireless technologies use. This spans all risks, including radicalization.

For this to happen effectively, we need better research. We need reliable information and studies on which educators and others in risk management can base their decisions. They need to be apprised of new trends and developing risks. They need to know that websites and services are using the latest and best technologies and have adopted the best industry practices with their users' safety in mind. They need help that Congress can provide by getting behind these research initiatives.

Congress can also be very helpful in helping gather relevant information about cybercrimes and abuses. I have testified previously that actual cybercrime 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.

Creating a central reporting database where all instances of cybercrimes are reported for statistical purposes, from radicalization sites and networks, to cyberharassment to Internet-related ID theft, fraud and scams, to sexual predators and Internet-related child pornography and sexual exploitation would be incredibly helpful. It could track cybercrime trends affecting adults, seniors and youth. It could be used to help design safer systems and best practices and guide legislation directed at a meaningful problem, in a meaningful way. This is the kind of centralized reportline that could be managed by the FTC or other governmental agencies.

In addition, with tax dollars becoming more and more precious and the mission of all Congressional representatives to put tax dollars into the most effective use, existing programs by trusted non-profit groups can be highlighted and made available online to schools and community organizations that need them, without cost. Without having to reinvent the wheel, massive amounts of programs, lesson plans and risks management guides already exist that can be used as is, or easily retooled. Finding a way to get these wonderful resources into the hands of those who need them the most, using interactive technologies and the Internet and mobilizing volunteers to help deploy existing programs that were developed with or without government dollars. Focusing attention on what works and what doesn't is something that Congress does best. WiredSafety.org and I pledge our help in doing that.

It's time. And hopefully, not too late.

APPENDIXES

1. Bio and CV of Parry Aftab, Esq.

2. Short Summary of WiredSafety.org's Programs

3. "Herding Cats" – Parry Aftab's Article for Thinkernaut, InformationWeek's expert blog group.

PARRY AFTAB

•Internet Privacy & Security Lawyer •Author •Award-Winning Columnist
•Consultant •Public Speaker •Child Advocate

OVERVIEW

Parry Aftab was one of the first lawyers in the world to practice Internet law. Over the years, she has represented many of the leaders from the entertainment, Internet and consumer brand industries. Known for her ability to "think outside of the box," she quickly became a leader in the emerging field of Internet law and policy and helped establish standards within the Internet industry. While she is an expert in risk-management issues across digital technologies for all demographics, most of her time is now devoted to issues and technologies impacting children and families online. Dr. Aftab is an award-winning columnist for Information Week magazine. She is also a frequent expert resource for, and quoted by, most leading media outlets around the world. Parry Aftab is a sought-after public speaker and has authored several books. When Internet policy, best practices and safety is involved, hers is the first name mentioned. Her expertise in social and community networking risk-management is in high demand and MySpace, Facebook, Xanga, Bebo and Piczo, among others, have turned to her for help.

ABOUT PARRY

Parry Aftab is a mother of two adult-children, resides in the NY metropolitan area, and maintains a home with her husband in New Brunswick, Canada. She started out on Wall Street in 1984 as a corporate takeover lawyer. Dr. Aftab completed her undergraduate degree in less than 2 years, as Valedictorian, with her two young children in tow. She is a member of Phi Beta Kappa and received her juris doctorate degree from NYU School of Law. Her work with children online followed her appearance on CNN in 1997, while discussing cyber-censorship. Shortly thereafter, confronted with evidence of child sexual exploitation online, she founded and continues to run the world's largest cybersafety and help group, now known as WiredSafety.org. Dr. Aftab works closely with regulators and law enforcement, the technology, entertainment and Internet industries, educational institutions and governmental agencies, worldwide, while donating her time running the charity. Parry Aftab carefully screens all new clients and limits her practice to enable her to devote a substantial portion of her time to child protection.

AREAS OF EXPERTISE

Parry Aftab is a legal and risk-management expert in all aspects of Internet best practices, privacy, cybercrime prevention and abuse-management. Her expertise extends to the traditional Internet industry, social and community networks, wireless and mobile technologies, cyber-marketing and interactive gaming. Because she works directly with thousands of young people and families online and in person each month, Dr. Aftab can provide a unique perspective and guidance on the design of technologies and marketing practices to address their needs. Since 1994, when she first began advising the Internet industry on children's and consumer issues, she has been called the "Kids Internet Lawyer." Ten years later, with the rising popularity of social networks and interactive technologies, Parry Aftab was the first to develop and promote the adoption of best practices for the Web 2.0 industry. Unlike other experts, Dr. Aftab's talents include her ability to blend practicality, safety and responsible business practices. She can also factor in societal, cultural and legal differences around the world. Those looking to build or protect their brands, globally, seek her advice first.

WHAT OTHERS ARE SAYING ABOUT PARRY

Parry Aftab was identified as "the leading expert in cybercrime in the United States," by the Boston Herald. Her "sound, balanced approach to children's online safety" was praised by The National Center for Missing and Exploited Children. She "understands what parents need and want to know," according to Stoyan Ganev, President of the UN General Assembly, 87th session. And Vinton Cerf, the "father of the Internet" calls Dr. Aftab "the quintessential, responsible Internaut." She has received numerous awards, including the Child Abuse Prevention Services Leadership Award and the 1998 President's Service Award from the Whitehouse. The US Congress formally honored her work in cybersafety in 2005 and in 1999 UNESCO appointed her to head up its online child protection project for the United States.

Parry@Aftab.com www.Aftab.com www.WiredSafety.org +1-201-463-8663

Parry Aftab's CV

Phone: 201-463-8663

parry@aftab.com

AREAS OF EXPERTISE: Web 2.0 compliance and risk management, Best Practices/ Worldwide Cybercrime Protection and Prevention, 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/ Cyberbullying/ Social Networking/ Privacy training and coaching

---

CURRENT POSITIONS

Cyber-Risk Consultant
Executive Director, WiredSafety.org (a 501(c)(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

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

President's Service Award – Whitehouse Award, 1998
For the charity she founded and runs

Singapore Broadcasting Authority,
PAGi advisory and founder of Cybermums

ORGANIZATIONS

Thinkernaut Expert – CMP (2007 – present)

NCPC Advisory Board – (2006 – present)

TRUSTe
Member- Board of Directors (Elected December 2002-2006)

Ad Council
Advisory Committee member (1999 - 2003)

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

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

The Internet Society
Elected Chair, Internet Societal Task Force and Societal Steering Group (worldwide, 2001)
Member of Public Policy Committee ISOC (2001–present)
Chair, Privacy and Security Working Group of The Internet Society Task Force (2000-2001) appointed member since 1999

WiredSafety (wiredsafety.org) the world's largest Internet safety and help group, formerly functioned as "Cyberangels," recipient of President's Service Award, 1998,
Executive Director (1998-present)

The National Urban League
Technology Advisory Committee (1997 – present)

AUTHORSHIPS AND RELATED ACTIVITIES

Author, selected books

Children and the Internet (official Chinese Internet safety guide)
China 2004

The Parent's Guide to Protecting Your Children in Cyberspace, McGraw-Hill, (U.S. edition, January 2000; UK edition, March 2000; Singapore edition May 2000 and Spanish language US edition November 2000)

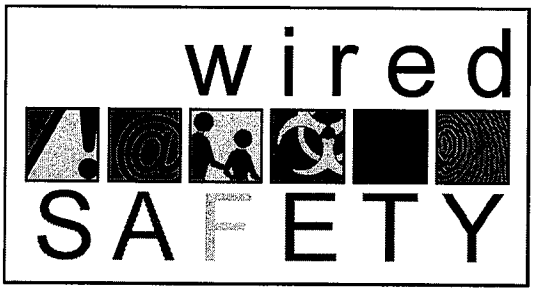
A Parents' Guide to the Internet, SC Press (October 1997)

Contributor, selected books

Child Abuse on the Internet.... Ending the Silence
(2001) Carlos A. Arnaldo, Editor
Chapter 21: The Technical Response: Blocking, Filtering And Rating The Internet - by Parry Aftab

The Best In E-Commerce Law
(2001) Warren E. Agin, Editor
Children's Online Privacy Law

wired
SAFETY



WiredSafety.org is the world's largest Internet safety and help group, comprised of thousands of unpaid volunteers. It is dedicated to helping families enjoy the new technologies, safely, privately and responsibly. Unlike other organizations which provide information and education alone, WiredSafety provides one-to-one assistance for victims of cyberabuse that may not arise to the level of a cybercrime and is not handled by law enforcement. Run by cyberlawyer, Parry Aftab, WiredSafety helps everyone stay safer online.

WiredSafety's cyberhelpline gives site visitors access to free help when they need it via the Internet. Its special team of helpline volunteers is assigned to cases and works one-to-one online to help resolve individual problems and get victims help when they need it. WiredSafety.org assists more cases of cyberharassment than any other organization in the world, helping thousands each month through its site and report line. Cyberbullying cases can be reported to the report line as well where parents and the cyberbullying victims can find a helping hand and knowledgeable help.

Its Teenangels, teen Internet safety expert program, is heralded by MTV, Teen People, Congress, Parliament and leading magazines, such as Prevention and Ladies Home Journal. Through their guidance children and other teens understand the consequences of risky online behavior. Through their consulting, the industry understands what young people want online.

WiredSafety runs WiredSafety.org, WiredKids.org, Teenangels.org, StopCyberbullying.org, Peers2Peers.org, Cyberlawenforcement.org and WiredCops.org, among other websites and programs.

Herding Cats

From CMP's Thinkernaut

Written by Parry Aftab

There was a time when any good Internet venture could be managed with some creativity, good editorial, financial know-how, and solid server maintenance. That was before massively popular social networking sites like MySpace , Facebook , YouTube Inc. , and the World of Warcraft came on the scene.

While there are many definitions of Web 2.0, mine is more simple than most. Before Web 2.0 technologies, sites communicated with the user. CNN, AOL, MSN, Yahoo, and others would post content and users would view it. Perhaps users would post a comment or two, or send an email, but it was essentially one-way site to user.

Web 2.0 bypasses the site, except as a conduit for user-generated content and direction. Instead of site-to-user (or user-to-world) content, it is user-to-user content. Web 2.0 technologies allow users to share thoughts, video, images, audio, and anything else -- real or imagined, true or false, good or bad.

In February 2005, I received a call from a friend whose 13-year-old niece had her full name, address, telephone number, school, and photo posted on MySpace.com. The entire family was upset and worried. I offered to visit his niece's school and speak to the students about cybersafety, and decided to reach out to MySpace and deliver a well-deserved lecture.

It took me a few hours to dig up a phone number for MySpace's corporate office. I called and asked for their general counsel's line. I was routed to his voicemail. I left a hateful message, telling him who I was, that I ran WiredSafety.org , one of the largest and oldest cybersafety help groups, and that we were watching them closely. I also dropped a bombshell. "By the way, you are out of compliance with COPPA." I never expected a return call.

When the general counsel called me back, I was shocked. "Parry, I know who you are and we need your help. We don't want kids on our site. We're designed for independent musicians between the ages of 18 and 34, not kids. It's like herding cats! Make them go away!" (Or, at least, that's the way I remember it.)

I told him I wasn't calling in cyberlawyer and risk management consultant mode. I was representing WiredSafety.org, which helps people, not businesses. He asked if we would point out things on MySpace that needed to be changed. If we did, he explained, millions of people would be safer in one fell swoop.

It was a novel approach, but it only had potential as long as I was willing to share my expertise for free, through the charity. But the carrot was keeping millions of people safer. I bit. Nevertheless, I needed to sell it to the volunteers acting as WiredSafety.org's key executives. Getting past the "sharing personal information online is dangerous" point was a real challenge, but it was essential if we were going to influence the creation of safer networks.

MySpace grew 1000 percent from 6 million users to 60 million within months. We were overwhelmed with requests for help. To their credit, MySpace reacted quickly when we made suggestions. They also fixed the COPPA problem within minutes. We helped institute privacy settings and better abuse reporting, and they adopted my pro-law-enforcement Investigator's Guide and procedures.

Other sites approached us, such as Facebook, Bebo, Piczo, and Xanga, and additional sites reach out daily. Even VCs and investors call us. Everyone wants their network be the poster child for safer networking.

Why did these and other leading sites turn to a cybersafety group to help them handle safety issues? It is because no company, regardless of how well-staffed and trained, is ready for what users of all ages will throw at them -- cyberstalking and harassment, ID theft, and underaged kids posing in the nude, to name a few problems.

Real or perceived anonymity by millions of unauthenticated users and lack of accountability is a serious risk management problem for sites. So, we've taken everything we learned about protecting kids and adults online, and merged that with old-fashioned risk-management, compliance, and privacy consulting and coaching. Early next year, with the first Web 2.0-support center, The WiredTrust will open its doors to teach companies how to herd cats, kids, and wayward adults. It will also allow networks to outsource moderation and abuse-management to have it done for them. Luckily for me, safety is now more than good business -- it's essential to staying in business. I knew if we hung in there long enough, things would come around.

— Parry Aftab, *Cyberlawyer, privacy and security expert, and Executive Director, WiredSafety.org (the world's largest and oldest cybersafety and help group)*

http://www.internetevolution.com/author.asp?section_id=469