JOINT COMMENTS
TO THE FTC

BY PARRY AFTAB, ESQ.,

WIREDSAFETY.ORG,

THE CHILD SAFETY RESEARCH AND INNOVATION CENTER

AND

WIREDTRUST, INC.

ON THE COSTS AND BENEFITS OF
THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT ("COPPA")
AND THE RELATED RULE

Submitted July 12, 2010

Parry Aftab, Esq.
201-670-7250
Parry@Aftab.com

Table of Contents

INTRODUCTION:

This comment is being jointly-filed by Parry Aftab, in her capacity as a child advocate, Internet privacy and security lawyer, and advisor to the Internet industry, WiredSafety.org, a US charity and the oldest and largest Internet and digital technology safety group in the world ("WiredSafety" or WiredSafety.org"), and WiredTrust, Inc., digital best practices and risk management advisors and the Child Safety research and Innovation Center, a Canadian non-profit.

Parry Aftab and the entities she represents have been active in the COPPA field and pre-COPPA kid's online privacy and safety space since 1994. She has advised and continues to advise the leaders in the Internet space, children's entertainment and game industries and trusted household offline brands on online issues. She helped frame COPPA and together with her former law partner, Nancy L. Savitt, provided extensive commentary on COPPA, represented the ESRB in their COPPA safe harbor application to the FTC and has written extensively on the subject of children, safety, privacy and best practices. Several of her previous comments and Congressional testimonies are attached to provide background on some of the challenges operators face under COPPA and changes in the industry since the 2000 implementation of the Rule. They are listed in the table of contents and also available at Aftab.com/COPPA.

WiredSafety is entirely run by grass-roots unpaid volunteers all over the world working from their computers, mobile devices and digital technologies providing help, education and awareness on cybersafety and privacy issues to all demographic groups, on all cyber-risks on all digital technologies and devices. WiredSafety's volunteers began by rating websites and providing help to victims of cyberbullying and cyberharassment in 1995. It operates, together with Parry, the most popular cyberbullying prevention website in the world, StopCyberbullying.org, and was selected as one of the five members of Facebook's safety advisory board and as one of 29 members of the Harvard Berkman Center's Internet Safety Technical Task Force ("ISTTF") formed at the request of 49 state Attorneys General to review social networking, risks to children online and available parental controls, safety and privacy-enhancing technologies. Recently WiredSafety was also represented through Ms. Aftab on the National Telecommunications Information Agency's Online Safety Technology Working Group ("OSTWG") appointed to render a report to Congress on data collection and management, child pornography reporting requirements, educational programs and parental controls. (That report was rendered June 4, 2010.)

WiredTrust is a for-profit consulting firm and represents the leaders in social gaming, online casual gaming, virtual worlds, social networking and family entertainment. Its clients range from general audience networks to the most popular children's websites and offline brands. WiredTrust conducts best practice, COPPA and compliance audits, certifies best practices and professional competences, delivers training for executives in risk management and for moderators and customer service personnel in cybercrime prevention, risk management, child protection and commonly-encountered abuses. It offers the only best practices seals in the industry and hosts conferences and workshops to help professionalize risk management for the digital technology, gaming and Internet industries. It has "in-the-trenches" experience in preventing and addressing risks online and building industry collaborations and cooperation and teams of preteens and teens to help advise its clients on trends and interests of other preteens and teens.

The Child Safety Research and Innovation Center is a Canadian non-profit dedicated to the development of learning applications and serious games to help children learn street-proofing, safer practices and ways to improve the world. It assists and advises governmental agencies, law enforcement and policymakers in North America and Europe on innovative technologies that enhance child safety, privacy and wellness.

All of the above entities and Ms. Aftab, in her individual capacity, offer their continued assistance to the FTC during this evaluation process and are happy to provide expertise or information at any time.

A. General Questions for Comment

1. **Is there a continuing need for the Rule as currently promulgated? Why or why not?**

   There is a continuing need for the Rule, but certain facets should be revised, updated and reconsidered. Safe harbors redesigned to provide broader best practices for children's websites, networks, sites and virtual world may be the way to adapt COPPA, as initially crafted, to address updated needs. (See Suggestions for the Next Generation of Safe Harbors below.)

   COPPA has been effective in creating awareness among Internet providers, interactive communication feature providers, digital technology providers, game providers and social networks about marketing, data collection and protection and safety. In 1996 CARU (the Children's Advertising Review Unit) developed the standards for marketing and advertising to children under 12 years of age in the US. When others identified unscrupulous and unfair practices relating to marketing and disclosures about what personal information was being collected and why, and the industry as a whole failed to respond to the FTC's voiced concerns, COPPA was born. In the ten years since its implementation, the industry has become far more aware of marketing best practices and more careful about what they do with preteens. Other privacy commissions and regulators around the world are looking to COPPA as a model for their own child protection and privacy laws. It has been effective in most of what it was intended to do. There are ways to improve it, some within the FTC's authority and some that may require Congressional action. But, as a whole, COPPA is necessary, and can help bring best practices to the kids Internet industry as a whole.

   That said, we need to identify more effective ways to engage parents, address their concerns as opposed to what we think might be of concern to them, understand the competing parental demands for their attention and find ways to reach them where they already are to get their cooperation. We need to reward innovation that addresses COPPA's underlying goals by creating safe harbors for the providers who adopt safer technologies and best practice standards. We have to help the industry find ways to become safer and more responsible and help parents identify the "good guys" online, who develop better and safer technologies and networks. Protecting children is good for business. We need to make sure that enforcement actions against those who ignore or fail to adhere to COPPA are brought when necessary and publicized. We must make it clear that it is cheaper in both the short and long run to comply with the law than thwart it. And we have to make it easier to comply, so more can afford to do it right.

   a. **Since the Rule was issued, have changes in technology, industry, or economic conditions affected the need for or effectiveness of the Rule?**

      More young people are using interactive digital technologies than ever before, in different ways than ever dreamed of. They are starting younger and younger and carry more digital power in their backpacks, pockets and purses than most corporations did twenty years ago.

      We were wired ten years ago. Now untethered, the concept of keeping the computer in a central location is as irrelevant and a slide rule in the days of calculators and computers. Online payment systems are more popular, allowing people without credit cards to engage in bank account and cash transactions online. The kids Internet industry had crashed in March 2000, before the

implementation of the Rule. No valid business models existed for kids online, other than advertising and promotional content that didn't support the costs of quality online content development and deployment. The middle tier of web companies in the kids' market had closed their doors, VCs refused to fund most kids sites because of the lack of financial success, and parents refused to pay for content online for their kids. (See Parry's 2000 COPPA Testimony for a background of where the industry was in October 11, 2000 when Parry Aftab testified before Congress on COPPA, a copy of which is attached hereto and available at Aftab.com/COPPA.)

COPPA was still a twinkle in the FTC's eye, in 1997 when the Center for Media Education first filed its complaint against Kidscom.com for unfair practices and failing to disclose what information was being collected from children and how it was being used, as well as failing to identify advertorials, as such, we had barely 10 million minors online in the US.

Cell phones were used to make phone calls and even then, only by business people and more affluent adults. Some teens had cell phones, usually passed down from their older siblings or parents, but they were the vast exception, not the rule. SMS was not in general use until 1999 – 2000 and then not by kids. Images were too large to send via a cell phone, no videos could be transmitted online without huge hosting costs and peer-to-peer networks were emerging as the way to share content (especially copyrighted music).

Virtual worlds were fringe or for adult-gamers. Chatrooms were popular online, instant messaging was ICQ and transitioning to AIM on AOL. Games were single-player or text-chat. Voice-over-IP was new.

Social networks didn't become mainstream until Winter 2004-5. Email was the most popular method of digital communication. Most children used DVD games, not online game networks. Handheld game devices were not interactive. Bluetooth or local communication connections were not in general use. Tweens were online far less than their teen counterparts and AOL kids-only parental controls were in broad use. High speed connections were rare and far slower than they are today. Videos could not be transmitted over traditional networks in real time. YouTube, Facebook, MySpace, Twitter, Google, Club Penguin, Xbox Live, PSP Network, texting, Webkinz and other global technologies and models were either not yet existent or fringe.

The world of kids online and using digital technologies from the age of three is new, with new risks, new challenges and new opportunities. Kids, tweens and teens live out loud online and on digital devices we never dreamed of 12 years ago.

There are many more ways to access the Internet than ever before and Internet-like technologies are becoming popular, as well. While anonymity was more important ten years ago, and "don't share any personal information online" was the mantra for everyone, especially minors, authentication, identification and understanding the risks and benefits of communicating with people we haven't met in real life and sharing certain limited personal information are on the rise and offer benefits to education, communication and community if managed properly.

This means we have to consider the initial needs addressed by COPPA, how it is still relevant in addressing those needs and any new information we have about those initial needs and newly identified ones.

The industry has changed substantially, as well. Not just the players, but their attitude towards collaborations and coalitions. Ten years ago, there was little cooperation among industry players. They often saw safety as giving them a competitive advantage. No one shared. Everyone built their own technologies and systems and kept their backends confidential. Trained moderators were rare and all moderators were discouraged from creating professional organizations and seeing themselves independent form their network employers.

At a recent WiredSafety event for its StopCyberbullying Coalition(which contains most industry leaders, the top experts in bullying and cyberbullying and member NGOs), a representative of Google interrupted a discussion where some of the industry members were promising to share their moderation and filtering technologies with others to improve safety across the board. "Safety is a competitive issue," he stated. Thinking that he was going to explain why Google would not join such an effort and instead creates proprietary safety systems of its own, Parry Aftab was pleasantly surprised to hear the rest of his statement. "If our competitors are safer, we need to be at least as safe." The days in which AOL and Microsoft didn't play well together are long gone. Much has been learned in the ten years since the Rule was implemented, but nothing more so than "we are stronger united than standing alone."

The government in the US and on a state-by-state basis has changed dramatically in their approaches to cybersafety and digital literacy as well. The Internet Safety Technical Task Force (the "ISTTF") administered by The Harvard Berkman Center was the first major task force formed in the US at the request of government to address cybersafety and children. Twenty-nine members (including WiredSafety) served without charge, paying their own expenses to help compile a report to 49 of the 50 state Attorneys General. That task force was followed by the National Telecommunications Information Agency's Online Safety Technology Working Group, appointed to review child safety online and related common industry practices and render a report to Congress. That report was submitted on June 4, 2010 and Parry Aftab, founder of WiredSafety, was honored to have been appointed to that working group as well. Government's expanding involvement will help, in turn, expand industry cooperation and commitments.

The industry leaders have also recognized the importance of formally tapping the expertise of the trusted cybersafety non-profits. Facebook named five international charities to its Safety Advisory Board (including WiredSafety), Microsoft's Xbox created a game safety advisory board, as did MTV. WiredSafety was asked to serve on those as well. McAfee created a consumer advisory board, chaired and founded by Parry Aftab, and others did as well. Working together is becoming the norm, not the exception and children and families will benefit.

These collaborations and cooperations are especially important when it comes to addressing COPPA and children's online privacy and safety. It will allow industry groups to develop industry-wide COPPA solutions, adopt safety moderation and filtering systems and agree on best practices that deliver COPPA goals at a reduced cost and are easier to implement. The whole industry can "find ways to put children first," quoting Dave Finnegan, Chief Technology Bear for Build-A-Bear Workshop at his recent cyberbullying testimony before Congress with Parry Aftab. Her testimony covered how much the industry is doing to help address cyberbullying, and is attached hereto as an addendum (Parry's Cyberbullying Testimony") and much of those same initiatives address children's privacy and general safety as well.

b. What are the aggregate costs and benefits of the Rule?

The costs of COPPA compliance are high, both in capacity-building and dollar and manpower demands. In some ways the costs have been reduced since the Rule's implementation, while in other ways they have increased. They are high enough that many providers will try to fit a size ten COPPA "foot" into a size five COPPA "shoe" by using a lower level of notice and/or consent for a higher risk. And since enforcement actions, while commendable, are still relatively rare, they can often get away with it. [1]This has the dual effect of exposing children to more risks, and making those sites cheaper to operate and therefore unfairly competitive with those seeking to comply with the Rule. And if the non-compliant site is popular enough to be seen as a "model" for under-funded start-ups, ironically its practices may be seen as safe and compliant because of whom they are and replicated. (This happens far more often than people realize.)

Exceptions are, of course, the easiest to administer once properly designed. Smart providers look to design as much as possible to fit into an exception rather than provide notices and obtain requisite consents.[2] The one-time use exception is inexpensive once the provider has conducted data-mapping and understands all points of online data collection (and if applicable, the combination of online collected data and online data collected from a preteen). They have to understand who receives the communications, equipment and software used and how they work, the location and mechanisms for all back-ups, if local copies are stored, communications are monitored using technology or other quality control systems and the process of responding to commonly encountered communications and exigent communications (in emergency situations). They must also know who has access to that data and provide training and processes that comply with COPPA for all such individuals.

If the provider receives an exigent communication "my daddy is hurting me," or "I don't want to live anymore," it can fall within the security and safety of the child exception or "We're going to launch a denial of service attack on your site," can fall within the security of the site exception. Then notices to the parent must be given (in the case of the safety of the child) or no notices have to be given (to protect the site itself) and the information stored and shared, if necessary.

Obviously, the more involved the applicable notice or consent mechanism, the higher the acquisition cost of consent.

Notice and opt-out methods are relatively inexpensive once the system is designed, the moderators trained and processes implemented. Higher costs come when the parent opts-out and the data must be deleted and the processes reversed. That typically involves manual systems, since it happens rarely.

If the site decides to track users whose parents have previously opted-out have an additional step to compare new applications with previously declines, either through the parent's email

[1] Like Ford in the Pinto case, the costs of compliance are weighed against the costs of non-compliance factoring in the likelihood of getting caught and penalized.

[2] The new approaches to chat are examples of ways in which providers are trying to design interactivity into exceptions, outside of "collection" of "personal information or reduced levels of consent to avoid the VPC high acquisition costs.

(0btained through their declining consent only, since once declined, the retention of either the child's or parent's information collected from the child is prohibited under COPPA.

The operator must always tag the user with the requisite consent received for future uses, as well. "Newsletters only" if the privacy policy and disclosures were limited for that purpose, "talking to Elmo" if they were defined that way, etc.

Verifiable parent consent options are limited, with the exception of credit card and paid subscription models, time consuming and often disruptive to the preteen's engagement. There is a low response experience and VPC methods are often misunderstood and misused.

In 2000, Parry Aftab testified before Congress about the effects of COPPA (see Parry's 2000 COPPA Testimony, attached hereto). At that time, she outlined the typical compliance costs (with offline verifiable parental consent models using fax and 800 numbers). In her testimony, Parry laid out the cost of COPPA compliance six months after its implementation. While the costs and processes are changed, the overall approach has not. It can be illustrative. (For the full text of her testimony, review the attachment.)

> "We have polled most of the mid-sized children's websites for the cost of COPPA-compliance, in hard dollars, not as to any lost revenue or loss in traffic. This can run from more than $115,000 per year to $290,000 per year, depending on whether the site is fully interactive, with chatrooms, etc. and what level of consent they collect. Here's what they told us:
>
> - $10,000 - 15,000 for legal, including audits and construction of privacy practices and policy
> - Cost of toll-free telephone and dedicated fax service [note: for obtaining verifiable parental consent in the days before an accepted paid subscription model]
> - $35,000 in engineering costs to make the site complaint
> - $2,500 - $10,000 monthly for professional chat moderators (price differs depending on training, hours of operation and organization)
> - $35-60,000 per year for one person to oversee offline consent, respond to parents= questions, review phone consents, and review permission forms.
> - $35-60,000 per year for person to oversee compliance, database security, respond to verification and access requests."

While these numbers are out of date, COPPA compliance costs continue to run high.

- Outside legal and privacy professionals should be engaged to look at the business models and goals and design a COPPA-compliant way to deliver on those models and goals. There are a handful of privacy professionals engaged in meaningful COPPA work, and these understand how children interact with technology, how parents can become engaged, the risks and ways to manage them. Without this holistic approach, COPPA is meaningless. The

fees for a true expert in COPPA can run between $15,000 to more than $50,000 on a one-time basis with ongoing advice being provided as needed and charged accordingly.

- Best practices audits for preteen sites, including COPPA compliance typically start at $25,000, with the better consultants charging $50,000 and up. COPPA safe harbor seals average $1500 annually and can run as high as ten times that for large networks with multiple privacy issues. Internal staff dedicated to COPPA compliance, high-risk communications, privacy and security troubleshooting and logistics can cost between $35,000 (for part-time low end staff) to $150,000 – $250,000 for a fulltime, in house chief privacy or compliance officer.

- Sophisticated database management professionals must be engaged to design a COPPA-compliant backend that allows for hashing of data, segmenting of data, scrubbing of data, access to all data relating to a single-user across the network or system, managing of passive data collection methods and email, feedback and abuse-management report data and authentication. They have to tag data for permitted collection and access relating to risks to the child herself, or to the network or site. This can start at $125,000 a year for a sufficiently experienced database designer and programmer and quickly increases from there. Outsourcing the design can cost from $60,000 to $185,000 and still require database personnel to maintain it and more design to adapt it to changing needs. This is over and above the cost of maintaining your data normally.

- Filters and moderation systems must be designed with COPPA in mind and the operators must weigh the desire to identify preteens on the network against the increased liability for monitoring of user-generated-content and online activities under the CDA. Protecting the anonymity of preteens is equally important as identifying them to protect them and others more effectively. Professionals can cost upwards of $50,000 for moderation and filtering design and process consulting. Training for moderators, including certification by trust third parties such as WiredTrust, costs $1500 for basic moderation training, including an introduction to COPPA. Moderation and filtering systems/technologies can run between $2500 and $15,000 per month, depending on the level of support and needs of the network and may also involve one-time customization charges ranging upwards of $50,000. Building your own, internally, may run upwards of $125,000 - $300,000 including your subject matter experts and licensing of filtered black list or white list terms and finding ways to make those lists work with your model and demographics may cost a further $10,000 - $15,000 to manage. Flagging new terms, risks and conduct to improve operations on an ongoing basis costs more.

- Human resources must ensure NDAs and company control of equipment used by moderation and customer service teams to comply with the privacy and security aspects of COPPA, and effective risk management requires background checks on all personnel having access to children's data and the children themselves. Monitoring technologies should be deployed to supervise compliance in moderation/customer service communications, including stripping of PII contained within one-time communications, while still logging the communications for data retention and risk management purposes. These can range from $200 - $5000 annually per moderator or customer service representative in addition to the ordinary costs of call centers, moderation centers or individuals.

- And in some cases, given the privacy and security requirements, outsourced providers in other countries may not be able to satisfy these requirements and more expensive providers in North America (Canada or the US) may have to be used instead. These increased costs, comparing a Filipino moderation provider at $6 per hour for outsourced moderation services to $12 an hour for a Canadian moderation provider, can be significant and result in the use of fewer moderators, a reduction of the hours during which moderators may be deployed or the use of less well-trained moderation teams, escalation teams and supervisors.

- Underage reports must be analyzed with the understanding that teens often target another teen in cyberbullying attacks by reporting them as underage and having the site do their dirty work unwittingly when the teen's profile or account is shut down. This, as well as pre-screening any user-generated-content or communications has to be done manually, using eyeballs and trained moderation staff to determine the credibility of a report and the likelihood that the user is underage given their friends, interests and other vague factors. When Parry Aftab first requested that MySpace use an algorithm to remove anyone they thought were underage, in early 2005, 300,000 profiles were removed. The result of using algorithms to do this was women who were "9" months pregnant, 40 year olds' profiles referencing memories of their middle and grammar school years and teachers of elementary aged students were inadvertently removed, to their owner's dismay.

- Challenges that can't be easily monetized include parents see the COPPA age-threshold as negotiable depending on their preteen's intellectual levels or sophistication and the confusion generated when we warn adults and children alike to not provide personal information unless they are sure of the trustworthiness of the recipient, and then ask them to provide credit cards to "okay" their child's use of a free site. Experts able to design a system that takes these and equally important factors into account are rare and expensive.

But there are significant enhancements to safety technologies created in response to COPPA as well. Ten years ago we thought COPPA would drive technology that would authenticate parents and perhaps preteens. While it didn't do that, in some ways it has driven more important safety technology and systems. Being able to avoid having to obtain VPC for a non-paid-subscription network or site is an important goal for most in the kids Internet industry. It is time-consuming, often interrupts the user-experience and the site's user-acquisition process, expensive and not very effective. It is, ironically, this high cost and manpower demand that has driven safer technologies.

The responsible sites want to comply with COPPA and care about the safety of preteens using their sites. Recognizing the realities of VPC compliance, though, they have created new systems that avoid their having to obtain VPC by prohibiting the sharing of personal information and keeping their users safer at the same time. Moderated and filtered systems, where the site operator can limit the terms, combinations of those terms and the methods of communications, tracks abuse reports, provide proactive review of user-generated-content postings, and moderate fora, games and chats are improving. Patterns of "grooming" behavior, suicidal threats, self-harm and cyberbullying communications can be analyzed and tracked to spot illegal and high-risk activities and identify troublemakers in the online systems, as we would in offline playgrounds. Kids can be enlisted to help patrol their own networks, as virtual hall monitors. And

triaged abuse-reporting user-interfaces can help get problems before those who can do something about them – user reports to site responses.

2. What effect, if any, has the Rule had on children, parents, or other consumers?

a. Has the Rule benefitted children, parents, or other consumers? If so, how?

Data collection and advertising practices have improved. Operators are now smarter about what they collect and how they use it. Networks and sites rarely engage in predatorial marketing to children or gather information that they don't need. Parents receive notice of some of their children's online activities. COPPA has raised awareness about best practices and has encouraged the development of safer more anonymous technologies. The safer technologies developed in response to COPPA, as described above are additional benefits.

b. Has the Rule imposed any costs on children, parents, or other consumers? If so, what are these costs?

Children, especially those whose parents don't have credit cards, may find themselves on the outside of a COPPA-compliant interactive website looking in. It has driven sites to charge for access to enable the use of credit cards for VPC that might otherwise have been free. Many advertisers avoid sponsorship or advertising on children's sites because of COPPA. Their sponsorship and advertising could have helped drive entertaining and valuable free content and activities.

Children must lie about their ages, since many sites prohibit use by anyone under 13 to avoid the costs and difficulties of COPPA compliance. Adults may not know they are interacting with a preteen when they are lying about their age. And the costs of COPPA compliance have to be spread among all subscribers, increasing costs for all users.

c. What changes, if any, should be made to the Rule to increase its benefits, consistent with the Act's requirements? What costs would these changes impose?

Finding ways to use the safe harbors to help bring consistent best practices standards and compliance to the industry can address Marketing Concerns, Safety Concerns and credibility at the same time.

3. What impact, if any, has the Rule had on operators?

a. Has the Rule provided benefits to operators? If so, what are these benefits?

The chief benefit of COPPA to operators is leveling the playing field between sites that do the right thing and others who don't. Those who adhere to best practices with tweens would be at a grave disadvantage when forced to compete with those who don't. Being able to receive safe harbor protection is also a substantial benefit to operators.

A side benefit to operators isn't COPPA itself, it is the stellar job the FTC has done to raise awareness and uncomplicate COPPA for operators with guides, FAQs and being accessible for questions. Phyllis Marcus jokingly referred to their accessibility to operators as the "1-800 call

Phyllis and Mamie Helpline." But everyone in the industry has a great deal of respect for them, their team and the FTC as a whole based on their work in COPPA.

b. Has the Rule imposed costs on operators, including costs of compliance in time or monetary expenditures? If so, what are these costs?

The costs and challenges imposed on operators by COPPA are multi-fold and high. More clearly defined below, COPPA requires the engagement of highly-experienced privacy or legal professionals,[3] sophisticated and well-defined data management, trained and supervised moderators and customer service representatives and systems, policies and processes. It is not for the weak and weary.

c. What changes, if any, should be made to the Rule to reduce the costs imposed on operators, consistent with the Act's requirements? How would these changes affect the Rule's benefits?

This issue is tricky. Most of the Rule merely addresses COPPA itself. It clarifies it, provides operational practicalities and guidance. Easing the challenges and costs imposed on operators can be effectively accomplished by industry coalitions, trade groups and collaborations to design, adopt and share technologies, methods of obtaining VPCs and Email Plus consents and practices. This can be codified under a new type of safe harbor that addresses best practices and provides the same or better protection than offered by the Rule to comply with the goals of COPPA.

4. How many small businesses are subject to the Rule? What costs (types and amounts) do small businesses incur in complying with the Rule? How has the Rule otherwise affected operators that are small businesses? Have the costs or benefits of the Rule changed over time with respect to small businesses? What regulatory alternatives, if any, would decrease the Rule's burden on small businesses, consistent with the Act's requirements?

The greatest area of growth of COPPA-applicable sites, networks and services are from the small business community. While the Disneys, Nickelodeons, and other entertainment and multimedia companies of the world control a significant portion of the preteen market online, small business founded virtual worlds, online games, social networks and preteen communities dominate the new site and service space. They may be the future Facebooks and Twitters, but today they are small, with fewer than 10 employees, funded from credit cards and home equity loans and struggling to build the technology, quick growth or decline, herd young kittens and figure out what laws apply to them and how to comply with those laws when they can't afford to buy a new coffee maker for the office. They care about kids' safety, and may have young children of their own. But they are caught between practical survival and the need to understand and address COPPA.

A relatively well-funded start-up in the kids interactive world space these days must have between $5 million and $10 million to get from proof of concept to the end of its first year. A few years ago, with fewer multimedia expectations and fewer platforms, a children's industry start-up could do it for between

[3] While COPPA information published on the FTC website makes compliance much easier than for similar privacy laws, COPPA is not a DYI-legal compliance project. Too many websites and operators have learned the hard way that their COPPA compliance is either too hot (overly-restrictive and unable to address their business goals and ability to deliver sites and services that can maintain a preteen's interest) or too cold, not adhering to the legal requirements and operational requirements of COPPA and using the wrong exception or method of providing notice or obtaining the requisite level of consent to comply with COPPA.

$2 million and $5 million, including the proof of concept development in most cases. But preteens are more sophisticated and more demanding now. They want chat and interactive communications. They want the opportunity to post their photos, interests and creative works. They want to use Facebook, YouTube and play online with millions of other kids their own age at the same time. They want 3D and a chance to change the world. The days when a tween site could avoid chat or user-generated-content are over, and that means all of these games, virtual worlds and sites have to comply with COPPA often with VPC, the most difficult of the consents to obtain and the most costly.

While a teen site, even for young teens, may be able to get by without black list filters and screening, a preteen site cannot do so and still pass parental scrutiny for long. There are no off-the-shelf products that they can buy to accomplish this. And existing filtering services can be costly and difficult to implement. Some, while well-meaning and designed to help comply with COPPA and safety needs, actual violate or facilitate the violation of COPPA by sharing and using data in ways not obvious or not disclosed by the operator.

They may use volunteer parents or teachers to moderate the site, often untrained and inconsistent in their responses. Their policies are decided, often, on-the-fly and honored in the breach. They may have the best idea in the world, but be in over their heads. The cyber fields are littered with the carcasses of failed children's sites. Not all, but some might have been able to make it if they had been able to bite the COPPA-bullet and understood how to make it all work within their business model.

The only way to help small businesses when COPPA is implicated is by the FTC providing webinars, workshops and tutorials to help them comply. Recent changes allowing for webcasting and offsite participation has broadened the reach of the FTC's panels and briefings. Model disclosures and templates that have been successfully used by others are helpful as well. Consultants who regularly advise the industry-leaders should provide information and resources on their websites, events and workshops and a COPPA-compliance-lite package, when possible, for small clients with limited budgets.

They should be able to access new technologies and tools that are in development, offering their expertise in exchange for reduced rates and guarantees. (Rather like the pioneer days or times of war, when everything contributed what they had to bake one cake and then received a piece of the cake for their contribution, WiredTrust is working with industry members of all sizes to create "Pathway" an overall moderation, risk and abuse management, filtering, reputational tracking and compliance technology that can be adapted to most digital communities' needs with minimal revamping. With the help of scientists and subject matter experts in Canada, child safety experts and operators from around the world, Pathway will tackle cyberbullying and harassment, sexual exploitation and grooming, ID theft, hate, lewd and hostile content and language for youth-oriented sites, advertising and marketing practices and risks associated with UGC, using semantic web and artificial intelligence technologies and science.

WiredTrust offers three levels of services for its best practices clients – we tell them what to do, help them do it or do it for them. Those on a budget can do more of the grunt work to get their policies written and practices implemented than those with the budget to outsource it all. Effectively-crafted intake forms can help a small business understand its choices and how a white-list quality chat system can avoid having

to obtain VPC from reluctant parents. COPPA by Design[4] can help them find the simplest path to their business goals while helping them comply with COPPA and protect their young users at the same time.

5. Does the Rule overlap or conflict with any other federal, state, or local government laws or regulations? How should these overlaps or conflicts be resolved, consistent with the Act's requirements?

In some ways COPPA currently is in tension with the Communications Decency Act's limitation of liability terms (the "CDA"). The CDA provides immunity from liability for what users do on a service provider's network, unless the service provider has direct control over that activity. Many states are seeking to pierce the CDA's protective shield, looking for ways the service provider may have overstepped its bounds as merely a service provider and become more of an editorial publisher liable for the actions of its users. The more the site does to make its fora, chat and UGC safer, the more vulnerable it may be under the CDA.

COPPA does not apply to a website has no actual knowledge that a preteen is sharing personal information on or having personal information collected by a provider, provided that the site is not directed at preteens. Constructive knowledge of underage users, absent more, if not enough to implicate COPPA. Should any changes be made to COPPA or under the Rule to change the standard from actual knowledge to constructive knowledge, the CDA will directly conflict with COPPA when provider liability is involved.

Different standards while not a conflict as such, can create confusion. Under the DMCA notice provided by a copyright holder, or on their behalf, that a user is infringing on that holder's copyrights makes the third party provider liable for copyright violations unless it takes certain affirmative actions to address the copyright infringements. COPPA-compliant providers, once credibly informed of the presence of an underage user without the requisite levels of consent, have "actual knowledge." But while the DMCA has clear guidelines on when a report of infringement should be believed and steps to take to confirm that the claimant has the requisite rights, COPPA has no such processes or methods of authentications. A teen can be manipulating the system to target a fellow teen in a cyberbullying attack, while posing as a concerned citizen of parent. COPPA should have more guidance on processes under the Rule.

a. Are there any unnecessary regulatory burdens created by overlapping jurisdiction? If so, what can be done to ease the burdens, consistent with the Act's requirements?

   Attorney General Abbott from Texas used COPPA to take action against a website he felt was unsafe, not for their privacy non-compliance but purely on their unsafe practices. While this doesn't appear to be a fast-moving trend, it can be troublesome for an operator who needs to understand the jurisdictional and substantive limits of COPPA.

   COPPA does not currently contain a pre-emption provision. It should.

b. Are there any gaps where no federal, state, or local government law or regulation has addressed a problematic practice relating to children's online privacy? Could or should any such gaps be remedied by a modification to the Rule?

[4] Using a phrase first coined by Dr. Ann Cavoukian, Commissioner of Information and Privacy for Ontario, Canada under her "Privacy by Design" brand..

The current laws and accepted industry best practice standards address things sufficiently in our opinion.

B. DEFINITIONS

6. **Do the definitions set forth in § 312.2 of the Rule accomplish COPPA's goal of protecting children's online privacy and safety?**

   Yes.

7. **Are the definitions in § 312.2 clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?**

   We believe that they are clear and appropriate.

8. **Should the definitions of ''collects or collection'' and/or ''disclosure'' be modified in any way to take into account online technologies and/or Internet activities and features that have emerged since the Rule was enacted or that may emerge in the future? For instance, how will the use of centralized authentication methods (e.g., OpenId) affect individual websites' COPPA compliance efforts?**

   We don't see Openid and other centralized authentication methods or services as a definitional issue. We see them as a way to facilitate notice and consent. The issues that have to be addressed in centralized authentication services is how to tie adults together with their children and how to verify that the adult is the child's parent with legal authority over that child.

9. **The Rule considers personal information to have been ''collected'' where an operator enables children to make personal information publicly available through a chat room, message board, or other means, except where the operator ''deletes'' all individually identifiable information from postings by children before they are made public and deletes such information from the operator's records.**

   a. **Are there circumstances in which an operator using an automated system of review and/or posting meets the deletion exception to the definition of collection?**

      Not practically. Small networks or sites with fewer than 500,000 registered users may be able to adopt this type of system, but sites with millions of active users cannot. The preteens are too good at gaming the system for the technology to adequately manage the pre-posting deletion/moderation quickly enough not to frustrate the user waiting for their post to appear.

   b. **Does the Rule's current definition of ''delete'' provide sufficient guidance to operators about how to handle the removal of personal information?**

      Yes, but most sites using this method fail to do it correctly. They may delete the information before posting, but still keep it on file without obtaining the requisite level of consent.

10. **Should the definition of ''collection'' be modified or clarified to include other means of collection of personal information from children that are not specifically enumerated in the Rule's current definition?**

We think that the Rule provides a broad enough description to include anything that is necessary without having to enumerated.

11. **What are the implications for COPPA enforcement raised by technologies such as mobile communications, interactive television, interactive gaming, or other similar interactive media, consistent with the Act's definition of ''Internet''?**

    We fall back on our approach to COPPA using the transparency test. Are parents sufficiently informed to understand what operators are doing, how they are doing it and the implications for their child's safety, privacy and security? Parents understand mobile phones. While they may not appreciate how many things you can do with them, they understand that you can use them to communicate in multiple ways, share and access content and buy things, as well as access the Internet, play games and download and listen to music, videos and other multimedia content.

    They may not understand the range of interactivity in online and handheld games, but should be asking the right questions before providing them to preteens. Several of the larger social and casual online game providers are discussing the need to label online games with a new form of rating applicable to small and social games, indentifying levels of interactivity, a simplified content rating system and the level of filtering/moderation for communications within the game. This may address some concerns of parents not fully familiar with interactive games. Some game devices are centralized, such as Microsoft's XBox, and COPPA-compliance is easier to accomplish at the one account entry point. Others, such as Sony's Playstation 3 has decentralized games which does not easily support an entry point COPPA-compliance model.

    Websites and services should have accessible privacy policies, settings and obtain the requisite consents however accessed. The fact that you can access them on your cell phone, other mobile device, desktop game device or handheld or interactive TV shouldn't be the issue. Cell phones are now capable of storing limited cookies in session and persistent formats. And parents can turn off these features any time they want.

    The rest, while increasing in use, are governed by other laws, regulations, best practices and industry standards or by parental awareness.

12. **The Rule defines ''personal information'' as individually identifiable information about an individual collected online, and enumerates such items of information. Do the items currently enumerated as ''personal information'' need to be clarified or modified in any way, consistent with the Act?**

    Not in our opinion.

13. **Section 1302(8) (F) of the Act provides the Commission with discretion to include in the definition of ''personal information'' any identifier that it determines would permit the physical or online contacting of a specific individual.**

    a. **Do operators, including network advertising companies, have the ability to contact a specific individual, either physically or online, using one or more pieces of information collected from children online, such as user or screen names and/or passwords, zip code, date of birth, gender, persistent IP addresses, mobile geo-location information, information collected in**

connection with online behavioral advertising, or other emerging categories of information? Are operators using such information to contact specific individuals?

Our clients are not, to our knowledge, using these methods to contact specific individuals. We cannot opine as to whether it is feasible or a commercially viable process. Existing profile, behavioral and sensitive marketing laws and models adequately address those issues without having to further encumber COPPA.

b. Should the definition of ''personal information'' in the Rule be expanded to include any such information?

No. If the FTC broadens the definition of "personal information" to include some of these, such as IP information, it will make it much harder to protect the safety of the sites' users and to track cybercriminals and protect the integrity of the site.

14. Are providers of downloadable software collecting information from children that permit the physical or online contacting of a specific individual?

Downloadable software, for these purposes can include undisclosed spyware, adware and tracking applications. These technologies should not be permitted on any site to which COPPA applies (or those to which is doesn't apply, in our humble opinion. The Socially Safe Seals both prohibit undisclosed spyware, adware or tracking technologies entirely.

Other downloadable software must be purchased and names, addresses, payment information and online contact information are customarily required at the point of online purchase. Most free software downloads require that you provide online contact information for the license.

The latest trend in gaming, games-to-Web applications, may collect GPS location data and share that with the game provider.

15. Should the Rule define ''the physical or online contacting of a specific individual,'' ''website,'' ''online service,'' or any other term not currently defined? If so, how should such terms be defined, consistent with the Act's requirements?

No.

C. NOTICE

16. Section 312.4 of the Rule sets out the requirements for the content and delivery of operators' notices of their information practices with regard to children.

a. Are the requirements in this part clear and appropriate? If not, how can they be improved?

Often the notice provisions are confused by the operators. Practical tutorials should be able to fix that easily.

b. Should the notice requirements be clarified or modified in any way to reflect changes in the types or uses of children's information collected by operators or changes in communications options available between operators and parents?

While it may not be able to be changed without Congressional action, notices and opt-out consent methods should be permitted for all uses other than third party marketing purposes sharing of personal information. It would result in fewer providers trying to circumvent COPPA, and therefore fewer children having to lie about their age to access those 13 and over sites.

Parents have the ability to limit their child's access to certain sites, monitor their activities online and prevent the sharing of personal information through the use of parental control technologies. They are becoming far more comfortable with their children's use of sites permitting user-generated-content and moderated chat.

Limiting the application of VPC to third party advertising and marketing shared personal information fits well within current parents expressed desires, needs and the lack of transparency that COPPA was designed to address.

D. PARENTAL CONSENT

17. Section 312.5 of the Rule requires operators to obtain verifiable parental consent before collecting, using, and/or disclosing personal information from children, including consent to any material change to practices to which the parent previously consented. This Part further requires operators to make reasonable efforts to obtain this consent, which efforts are reasonably calculated to ensure that the person providing consent is the child's parent, taking into consideration available technology.

a. Has the consent requirement been effective in protecting children's online privacy and safety?

The only effective method for obtaining verifiable parental consent ("VPC") is through paid subscription websites and services which charge a credit card, online service (such as PayPal or Facebook Connect-type technology) or use a "check-equivalent" or other financial institutional method. The others are slow, ineffective, and difficult to administer and have not been broadly adopted.

The VPC methods designed to provide parental consent are a bit of a fiction. They are designed to obtain consent from an adult, not necessarily the parents or even the custodial parent. But it was the best the FTC could and still can do, under the circumstances. Methods proposed to obtain consent via schools that identify the legally-responsible parent or legal guardian have failed to address FERPA concerns, the liability of the school and ways to get them engaged in helping facilitate the commercial use of the Web. They haven't delivered on the promise of getting the one broadly-capable system to authenticate preteen students and their parents. Proposals for large databases of preteens and their parents are more frightening than helpful, in our opinion. Proxy-consent mechanisms should work, if a trusted third party can be identified to verify parental authority, and the adoption rate is high enough. (But many larger providers do not want to share the valuable data they get by working directly with the parents and don't want to share their "edge" and customer acquisition lead.)

Other problems arise in VPC systems. What about all of those without credit cards or online payment accounts (such as PayPal)? Are those preteens locked out of COPPA VPC networks? Are they prohibited from using chat or posting user-generated-content? Do their parents have to resort to fax, print-and-mail, or out-of-date telephone call verification systems? Do they have to wait a week to get their user name and password?

COPPA currently has the unintended consequence of allowing more affluent children access to services and online activities than their less-privileged counterparts. That has to be addressed. This is as much an issue of accessibility as broadband. The Internet is the great equalizer, except when interactive communications and preteens are involved. For that, we need easier and a wider range of VPC methods.

b. What data exists on: (1) operators' use of parental consent mechanisms; (2) parents' awareness of the Rule's parental consent requirements; or (3) parents' response to operators' parental consent requests?

One-Time Use Exception – If the site, service or network receives a communication online that is a single inquiry, not tied to previous inquiries or other information you have collected on that preteen, and you do not store the personally identifiable information provided by that preteen, no notice has to be sent to parents, not consent is required. (Obviously, the privacy policy has to otherwise comply with COPPA's requirements, if applicable.) Parents would not be concerned about a commercially-responsible operator or provider answering a one-time question and not collecting information from their child.[5] WiredSafety's polls reflect that 96% of parents had no problem with their preteens asking a one-time question and getting an answer from a site, network or game provider without being informed by the site, network or game provider.

Online Contact Information for Multiple-Use Exception – This exception is most easily understood if you separate online and offline contact information in your analysis. If all you are collecting is the preteen's email address and not combining it with any other personal information (full name, postal address, mobile or phone numbers, etc.) other than the parent's email address, you can have multiple communications with the preteen user. This is most commonly used with newsletters, alerts about new activities and regularly-scheduled communications going from the provider to the preteen. Here, the parents receive notice via email sent to the email address collected from the preteen. The notice, *inter alia*, must include the information being collected, how it is being used, links to the privacy policy and the ability to opt-out on behalf of their preteen. This too makes sense. Parents may want to know, but not necessarily want to have to take affirmative action to consent to their preteen's subscription to a newsletter at a commercially-responsible site/network/provider. Email works for this purpose, and given the low level of risk at a COPPA-applicable commercially-responsible operator, the notice not getting delivered isn't a serious problem. Parents have informed WiredSafety that they appreciate the notice, but rarely read it and never opt-out. They don't particularly care if they are informed about newsletter signups, etc.

[5] Backend issues exist with offsite moderators and customer service personnel using their own equipment, often retained without background checks, training or supervision. "Commercially-responsible" is measured under accepted best practice standards for those working with preteens and children. The Socially Safe Kids Seal and related best practices audits address these and similar process and system risks and practices.

Many providers confuse this consent level and use it to notify parents when they are collecting multiple types of information from their preteens, instead of the Email Plus method required under those circumstances. They sometimes even try and use it when open-chat is offered at a site, or user-generated-content is permitted without full white list technologies or pre-screening without understanding the full-fledged verifiable parental consent requirement for such capabilities.

The notice and opt-out works very well if the parent's real email is provided by the preteen. The emails need to get through as well. Even with the correct email, with network-level SPAM filters and those employed on the local machine level, many emails never arrive at their intended destination. Once these two issues are addressed, this method has substantial promise.

Requiring opt-in is a problem.[6] Parents often don't have the time, or inclination, to provide consent to a site. They have been taught to distrust online communications asking for opt-in or them to take some sort of action. Initially we concluded that parents didn't provide consent because they didn't want their preteens engaged in those activities with that operator. But experience has taught us otherwise.

Finding ways to broaden this method of providing notice to other applications, in a safer filtered environment, perhaps, will help promote COPPA-compliance and obtain parental involvement. This can allow preteens to use a commercially-responsible site or network without having to wait for their parent to give permission.[7]

Email Plus – Initially designed to get the industry over the hump of finding ways to digitally authenticate parents in 2000, the FTC adopted "Email Plus" when the safety risks are deemed relatively low and personal information is not shared outside of the provider or posted for third-parties to see. It was designed for Marketing Concerns, exclusively, but has some practical

[6] "Parents care about privacy and online safety, but they aren't interacting with the sites or supporting the sites that protect their children's safety and privacy. It may be that they are intimidated, or just plain too busy. But the children's online laws depend on obtaining parental consent, and if parents aren't bothering to provide consent, sites are running into problems.

Bonus's experience is a case in point. It found that out of the parents who were asked for their consent for Bonus to use children's information internally, 51% never replied, 31% provided consent and 5% said "no." (13% are still pending from this sample group.) This was a six to one ratio of parents allowing their children to use those services, over those who wouldn't allow them to share the information. But the 51% of parents not bothering to respond is frightening.

Bonus is losing more than half of the children who want to participate. And Bonus doesn't have chat, e-mail, e-commerce, on instant messaging. Bonus is a site that has games for children, and sends newsletters to their site visitors. This is a typical situation faced by many children's sites."
Quoting Parry's 2000 COPPA Testimony (see below).

Ten years later, little has changed other than for the closing of Bonus a few years ago.

[7] In Parry Aftab's testimony before Congress in connection with the implementation of COPPA on October 11, 2000, she discussed the cost of COPPA compliance and the slow adoption of parental verifiable parental consent methods. (See Parry Aftab's Testimony before the U.S. House of Representatives, Committee on Commerce, Subcommittee on Telecommunication, Trade, and Consumer Protection, October 11, 2000 attached hereto (the "Parry's 2000 COPPA Testimony".)

applications with the Safety Concerns as well. We all assumed it would be phased out once digital signatures became broadly used. But when new authentication models and technologies failed to gain in parental adoption, it was continued and is in broad use for one reason – it's simple. If a provider wants to start pairing online contact information with offline contact information and broader regular communications, especially in marketing of the provider's services and doesn't share this with third parties, this method of consent is still available.

This level of consent, however, is the most confused and most abused (largely because of the confusion). Most providers understand the need not to share personal information they have collected from a preteen user with third-parties. They understand the Marketing Concerns pretty well. But they don't understand the Safety Concerns and how user-generated-content, chatrooms and fora and online communications implicate COPPA and what they have to do to notify parents and obtain the requisite level of consent from parents. They expect that an online method using email would be available and this seems to fit expectations.

Parents are never crazy about marketing (few are). They are not particularly happy with anyone promoting anything, even their own products and services, to their preteens. And the more personal information the marketer/provider has about the preteens, the less parents like it. At the same time, many sites still operate on a "marketing" model promoting products or services or building brand recognition and loyalty. That means, unless we are going to drive all sites and operators to a subscription model or only allow preteens whose parents have credit cards or disposable income to use the site, we have to address this reality. Many quality sites, virtual worlds and networks can remain free if a responsible internal marketing solution can be identified.

Smarter providers don't pair unnecessary personal information with online contact information if they don't have to. You don't need to know Johnny's last name to promote sporting goods to him, but knowing his zip code is helpful to identify the right kinds of sports and weather-related sportswear. The zip code is also helpful to identifying sports teams and location of sporting events. It makes the communications more relevant. It provides value in ways marketing messages without zip codes can't. If they don't combine information, the notice and opt-out method (Online Contact Information for Multiple-Use Exception) might work better, be cheaper to manage and streamline their consent/compliance process.

The difficulty of getting parents to take affirmative action or respond to a link in an email to consent to their preteen's use of a website, game or online network is a reality that is forcing many operators to find a way around COPPA or pretend no preteen users are allowed on their sites.

Verifiable Parental Consent – Verifiable parental consent is not email. It requires a higher level of authentication to demonstrate the likelihood that the person providing the consent is the preteen's parent.[8] But even if this has been overcome, VPC's weren't working. In previous testimonies and on

[8] The VPC methods designed to provide parental consent are a bit of a fiction. They are designed to obtain consent from an adult, not necessarily the parents or even the custodial parent. But it was the best the FTC could and still can do, under the circumstances. Methods proposed to obtain consent via schools that identify the legally-responsible parent or legal guardian have failed to address FERPA concerns, the liability of the school and ways to get them engaged in helping facilitate the commercial use of the Web. They haven't delivered on the promise of getting the one broadly-capable system to authenticate preteen students and their parents. Proposals for large databases of preteens and their parents are more frightening than helpful, in our opinion. Proxy-consent

FTC panels since before COPPA was adopted, Parry Aftab has repeatedly explained that verifiable parental consent wasn't workable unless and until a paid subscription model for the preteen Internet industry emerged. Until Disney's Club Penguin caught on five - six years ago (a year prior to its acquisition by Disney), the paid subscription model wasn't viable. Everyone trying it either changed their business models or closed their doors. But the demand for Club Penguin by the preteens themselves and the resulting "nag factor" gave COPPA a new life. Obtaining verifiable parental consent ("VPC") when a credit card or other financial transaction is involved is easy and just one more step in the payment process. It reduced the cost of obtaining a compliant VPC from $45 - $108 per initial consent to barely more than the cost of legal advice and system design spread over the size of the preteen subscriber-base – virtually pennies.

While not all sites, networks or games require a paid subscription, the use of payment mechanisms has become very common and more acceptable. For the preteens whose parents have credit cards or online payment accounts, COPPA full-fledged VPC is attainable. (Many operators don't understand that it is not the fact that a credit card exists that provides acceptable verification, it is the actual charging of the card so the parents can see the charge on their monthly statement that is required.)

But what about all of those without credit cards or online payment accounts (such as PayPal)? Are those preteens locked out of COPPA VPC networks? Are they prohibited from using chat or posting user-generated-content? Do their parents have to resort to fax, print-and-mail, or out-of-date telephone call verification systems? Do they have to wait a week to get their user name and password?

COPPA currently has the unintended consequence of allowing more affluent children access to services and online activities than their less-privileged counterparts. That has to be addressed. This is as much an issue of accessibility as broadband. The Internet is the great equalizer, except when interactive communications and preteens are involved. For that, we need easier and a wider range of VPC methods.

Ten years ago we thought COPPA would drive technology that would authenticate parents and perhaps preteens. While it didn't do that, in some ways it has driven more important safety technology and systems. Being able to avoid having to obtain VPC for a non-paid-subscription network or site is an important goal for most in the kids Internet industry. It is time-consuming, often interrupts the user-experience and the site's user-acquisition process, expensive and not very effective. It is, ironically, this high cost and manpower demand that has driven safer technologies.

18. **Section 312.5(b)(2) of the Rule provides a non-exhaustive list of approved methods to obtain verifiable parental consent, including: providing a consent form to be signed by the parent and returned to the operator; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; and using email accompanied by a PIN/password obtained through one of the other enumerated verification methods.**

---

mechanisms should work, if a trusted third party can be identified to verify parental authority, and the adoption rate is high enough. (But many larger providers do not want to share the valuable data they get by working directly with the parents and don't want to share their "edge" and customer acquisition lead.)

a. To what extent are operators using each of the enumerated methods? Please provide as much specific data as possible, including the costs and benefits associated with each method described.

Parry Aftab and Nancy L. Savitt developed the first 800 number consent mechanism. It was designed for Headbone, a formerly popular website no longer operating. The challenge was making sure that the parents had printed out the instructions from the site in advance, since dial-ups were still the most used method of connecting to the Internet at that time and they needed to use the phone to make the call. Kids would call posing as their parents, leaving messages stating that "Hi, I am my father and I said it's okay to sign up for Headbone." Every day it was an adventure.

Neopets is one of the few providers still using the print and fax or mail methods, largely for legacy purposes. The tweens think it is special just to Neopets.

Most, when they can, use credit cards either charging them or not, without understanding the legal requirement to charge them as well as the merchant account issues in using them only for authentication without charging them.

b. Are there additional methods to obtain verifiable parental consent, based on current or emerging technological changes, that should be added to § 312.5 of the Rule? What are the costs and benefits of these additional methods?

The Rule permits any method that is sufficiently reliable. In our opinion, the list is not limited to the enumerated methods. In our opinion, the more methods that can be identified, the better. What may work for a small business may not work for a large multi-million user game network.

Proxy consent services that use set parameters and standards (such as those available under a best practices safe harbor program) to allow a parent to verify their identity one time and give instructions to the proxy consent service to provide consent to sites and services that meet that criteria, on that parent's behalf. The one-time VPC acquisition cost is shared among all member sites and services and if that proxy consent service provider is a non-profit or charity and receives the small charge used to satisfy the credit card or other payment mechanism VPC requirements, everyone benefits. WiredSafety is weighing whether it should create such a system.

Paypal charges are being used with greater frequency as a VPC method. And schools are getting involved as well, although not as effectively as we had anticipated.

Many new methods are seeking to use the cell phone's payment technologies and text services, Facebook Connect and other similar methods to provide at least Email plus consents and in some cases VPC.

c. Should any of the currently enumerated methods to obtain verifiable parental consent be removed from the Rule? If so, please explain which one(s) and why.

While some are outdated, all are acceptable.

d. Are there methods for delivering a signed consent form, other than postal mail or facsimile, that would meet the Rule's standards for verifiable parental consent? Should these be specified in the Rule?

Scan and email, with confirmation of receipt, while costly and hard to manage by the operator is an easy reach from existing print and mail methods.

e. **Are there current or emerging forms of payment, other than the use of a credit card in connection with a transaction, that would meet the Rule's standards for verifiable parental consent? Should these be specified in the Rule?**

Virtual checks, electronic bank account withdrawals, Paypal and equivalent online financial accounts including iTunes are either in use or being contemplated.

f. **The Rule permits use of a credit card in connection with a transaction to serve as a form of verifiable parental consent. Is there data available on the proliferation of credit cards, debit cards, or gift cards among children under 13 years of age? What challenges, if any, does children's use of credit, debit, and/ or gift cards pose for Rule compliance or enforcement?**

While many more preteens have access to credit cards, online payment services (like Paypal), iTunes allowance accounts and other financial mechanisms than before, and parents still oversee most purchases or review the month-end statements.

The recent acceptance of the paid subscription models and purchases of virtual goods has made this a much more effective method with a high rate of adoption and a relatively inexpensive cost of acquisition.

g. **Are there current or emerging forms of oral communication, other than the use of a toll-free telephone number staffed by trained personnel that would meet the Rule's standards for verifiable parental consent? Should these be specified in the Rule?**

While technologies that claim to identify the age of someone by their voice alone may be scientifically feasible, it is not commercially feasible for COPPA purposes to our knowledge.

19. **Section 312.5(b) (2) also sets forth a mechanism that operators can use to obtain verifiable parental consent for uses of information other than ''disclosures'' (the ''email plus mechanism''). The email plus mechanism permits the use of an email coupled with additional steps to provide assurances that the person providing consent is the parent, including sending a confirmatory email to the parent following receipt of consent or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. In 2006, the Commission announced that it would retain the email plus mechanism indefinitely. See (http://www.ftc.gov/os/ fedreg/2006/march/060315childrens- online-privacy-rule.pdf).**

a. **Does the email plus mechanism remain a viable form of verifiable parental consent for operators' internal uses of information?**

It is a preferred method of VPC when internal marketing use is an objective. It is often confused, however, by operators thinking it is a viable method of obtaining VPC for open communications and posts or third party sharing of information.

b. **Are there other current or emerging forms of communications, not enumerated in § 312.5(b) (2), that would meet the Rule's standards for verifiable parental consent for operators' internal uses of information? Are any changes or modifications to this Part warranted?**

Facebook Connect and similar technologies, text and Blackberry Messenger technologies have promise. Expanding the Rule to make it clear that other email-equivalents apply whenever email is identified as a method of providing notice or consent.

E. EXCEPTIONS TO VERIFIABLE PARENTAL CONSENT

20. COPPA and § 312.5(c) of the Rule set forth five exceptions to the prior parental consent requirement. Are the exceptions in § 312.5(c) clear? If not, how can they be improved, consistent with the Act's requirements?

Our comments to exceptions and methods of notification and obtaining consent as set out in greater detail above.

21. Section 312.5(c)(3) of the Rule requires that operators who collect children's online contact information for the sole purpose of communicating directly with a child after the child has specifically requested such communication must provide parents with notice and the opportunity to opt- out of the operator's further use of the information (the ''multiple contact'' exception).

a. To what extent are operators using the multiple contact exception to communicate or engage with children on an ongoing basis? Are operators relying on the multiple contact exception to collect more than just online contact information from children?

Operators love the multiple contact exception without understanding that it is not permitted for marketing to kids. Its limited application is almost always ignored or misunderstood.

That said, allowing the newsletter to include marketing messages or permitting the operator to send out alerts about new products or services under this exception is something that should be considered.

b. Should the multiple contact exception be clarified or modified in any way, consistent with the Act's requirements, to take into account any changes in the manner in which operators communicate or engage with children?

Allowing the collection of a preteen's cell number solely for the purposes of delivering the newsletter via text makes sense and should be permitted.

c. Under this part, acceptable notice mechanisms include sending the opt-out notice by postal mail or to the parent's email address. Should § 312.5(c) (3) be modified to remove postal mail as a means of delivering an opt-out notice to parents?

Why? Although not frequently used, if it helps some parents provide opt-out it should be permitted. The operators who wait sufficient time to see if the parent opts out using this method may find that it doesn't meet their need or the needs of the child.

d. Should § 312.5(c)(3) be otherwise clarified or modified in any way to reflect current or emerging technological changes that have or may expand options for the online contacting of children or options for communications between operators and parents?

No.

22. Section 312.5(c)(4) of the Rule requires an operator who collects a child's name and online contact information to the extent reasonably necessary to protect the safety of a child participant in the website or online service to use reasonable efforts to provide a parent notice and the opportunity to opt-out of the operator's use of such information. Such information must only be used to protect the child's safety, cannot be used to re-contact the child or any other purpose, and may not be disclosed.

a. To what extent, and under what circumstances, do operators use § 312.5(c) (4) to protect children's safety?

Subsection (4) provides:

"Where the operator collects a child's name and online contact information to the extent reasonably necessary to protect the safety of a child participant on the website or online service, and the operator uses reasonable efforts to provide a parent notice as described in Sec. 312.4(c), where such information is:
(i) Used for the sole purpose of protecting the child's safety;
(ii) Not used to recontact the child or for any other purpose;
(iii) Not disclosed on the website or online service."

This provision is used more often than most people outside of the children's Internet space realize. When preteens interact regularly with a site, network or virtual world or game site, they often turn to moderators or customer service representatives as "trusted adults." In addition to cyberabuses, cyberbullying and other online risks they may encounter, children may seek help for offline bullying attacks, problems with school or even cases of parental/child abuse, parental drug or alcohol abuse or financial problems or martial breakups. COPPA gives operators no leeway in the collection of the child's contact information to the extent reasonably necessary to protect the safety of a child on the website or online service and, under this exception requires notice be given to the parents.

Although it relates expressly to the child's safety on the site or service, many providers read this more broadly and use it to authorize the collection and use of the child's name and online contact information when the child's safety online or offline is implicated. Without this read, the child may find themselves with no place to turn, especially if the child is at risk at home. Problems exist outside of the broader read and stretching of this exception, as well. How can an operator provide notice to the parent if the child shares information that may cause the operator to believe that by doing so the child could be put at risk?

b. Are the requirements of § 312.5(c)(4) clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?

The language is clear, although without broad child safety application unless it also applies to children at risk wherever that risk arises that is provided by that child or by another child to the operator. This provision should be expanded to permit the operator to collect name and online contact information, as well as offline contact information, including their school and, if applicable, both parents' contact information, if they believe that the child is at risk or poses a risk to themselves or others. Without this, the operator is not permitted to collect online or offline contact information for a parent to inform them that their child has threatened suicide following a cyberbullying incident that occurred on another site or has made allegations of school abuse. This is unconscionable. If subsection 4 cannot be broadened, some way must be found to permit the operator to play a role in protecting their child users within the confines

of COPPA without risking liability for doing so. The exception could still be confined carefully on permitted use and disclosures and children will be safer.

23. **Section 312.5(c)(5) of the Rule permits operators to collect a child's name and online contact information to protect the security or integrity of the site, take precautions against liability, respond to judicial process, or to provide information to law enforcement agencies or in connection with a public safety investigation.**

    a. **To what extent, and under what circumstances, do operators use § 312.5(c) (5)?**

    Operators use subsection 5 to protect themselves and sometimes to cover when an overly restrictive privacy policy prohibits exigent circumstance disclosures to law enforcement. To protect themselves against ankle-biters, trolls and young hackers, code and cheat schemes, in cases of posers, account takeovers and point and item thefts, break-ins and account intrusions, this exception is essential. Here, unlike in subsection 4, no notice has to be given to parents before the information is collected, stored or shared with law enforcement agencies or to protect the public. This exception also covers malicious code attacks and can be used to address large scale cyberbullying when the bullies are the members of the network. Typically the targets are covered by subsection 4.

    b. **Are the requirements of § 312.5(c) (5) clear and appropriate? If not, how can they be improved, consistent with the Act's requirements? For example, should § 312.5(c)(5) of the Rule be clarified to allow operators to collect and maintain a child's name and/or online contact information for the purpose of preventing future attempts at registration?**

    This subsection is the only provision of COPPA that allows the operator to protect itself and others. The need to allow an operator to collect and share information necessary to the safety of a child on or off of the operator's site or service can be as easily added to this subsection as subsection 4, especially if the parent is the accused and notice cannot be given without putting the child at risk.

    As suggested, for operators willing to collect and store IP information, MAC numbers, preferred screen names, email addresses, names and similar indicators to spot children seeking to reapply for membership if previously either denied membership or having had their membership terminated or suspended, this exception should be expanded.

    WiredTrust is hosting a by-invitation-only high-level best practices and online games and social networks event in October 2010 to help address common questions, risks and find solutions when needed for the industry as a whole. The FTC is welcome to participate at this event to gather additional information as to the kinds of information the operators need to better protect their sites, the public and prevent cybercrimes and abuse.

F. Right of a Parent to Review and/or Have Personal Information Deleted

24. **Section 312.6(a) of the Rule requires operators to give parents, upon their request: (1) a description of the specific types of personal information collected from children; (2) the opportunity to refuse to**

permit the further use or collection of personal information from the child and to direct the deletion of the information; and (3) a means of reviewing any personal information collected from the child. In the case of a parent who wishes to review the personal information collected from the child, § 312.6(a)(3) of the Rule requires operators to provide a means of review that ensures that the requestor is a parent of that child (taking into account available technology) and is not unduly burdensome to the parent.

a. **To what extent are parents exercising their rights under § 312.6(a) (1) to obtain from operators a description of the specific types of personal information collected from children?**

   Since the privacy policy should contain this information, parents may not feel the need to request this information. In our experience and the experience of our clients this information has not been requested from them.

b. **To what extent are parents exercising their rights under § 312.6(a) (2) to refuse to permit the further use or collection of personal information from the child and to direct the deletion of the information?**

   Over the ten years that Parry Aftab or any of her practices or consulting firms have served the children's Internet industry or the trusted brand community by providing COPPA advice or best practices consulting, only four cases have been reported to her of parents seeking the deletion of information collected from their child or to review the information collected from their child. In each of those cases, the information was sought by the non-custodial parent to confront the custodial parent about their child's Internet usage. In three of those cases a custodial battle was ensuing and their lawyer had advised them to seek this information.

c. **To what extent are parents exercising their rights under § 312. (a)(3) to review any personal information collected from the child?**

   See (b) above.

d. **Do the costs and burdens to operators or parents differ depending on whether a parent seeks a description of the information collected, access to the child's information, or to have the child's information deleted?**

   Yes. A well-drafted privacy policy will contain the description of what information is collected from a child, how it is used, with whom it is shared, how it is stored and secured and what choices are available. Any inquiry relating to what kind of information is collected from children can be addressed merely by reference to the privacy policy.

   The chief challenges and costs relating to parental requests for their child's collected and stored information relate to the authentication of the parent or legal guardian, verification of their right to access their child's information outside of the blanket COPPA authority (particularity for non-custodial parents, birth parents, parents with severed parental rights, etc.). Legal standards for guardians and parents differ by legal jurisdiction and radically by country customs and laws. The operators are rarely in the position of authenticating both the parent or legal guardian and

verifying their legal standing on a global basis. The safe harbor for operators under Sec 312.6(b) [9] is an important step to limiting the operator's liability for good faith disclosures. But without the permitted disclosure provisions in the privacy policy, the operator may still be liable for mistaken disclosures under civil litigation and breach of contract claims. So, our clients are always advised to include broad provisions in their privacy policies covering disclosures made in good faith to protect the site, comply with applicable law, protect the child, the general public or other users.

Parry Aftab advises her clients to seek input from the child's school when these requests are received, after having provided the parent making the request with their authentication and verification processes which includes their consenting to the school being contacted and providing the contact information for the school and completing a notarized FERPA-compliant release in favor of the school and the operator. Since this happens so rarely and generally the operator has someone or a team of customer service personnel to handle complaints of posers, infiltrated accounts and account takeovers manually, this imposes little additional costs or risks.

The information deletion process is trickier. The more the operator anonymizes their processes, posts and data shared, posted or used, the harder it will be to locate that data for deletion upon the authorized parent's request.

e. Is it difficult for operators to ensure, taking into account available technology, that a requester seeking to review the personal information collected from a child is a parent of that child?

Absolutely.

f. Should § 312.6(a) (3) enumerate the methods an operator may use to ensure that a requestor seeking to review the personal information collected from a child is a parent of that child? Should these methods be consistent with the verification methods enumerated currently or in the future in § 312.5(b) (2) of the Rule?

It should provide guidance and examples.

g. Are the requirements of § 312.6 clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?

Yes.

G. Prohibition Against Conditioning a Child's Participation on Collection of Personal Information

25. COPPA and § 312.7 of the Rule prohibit operators from conditioning a child's participation in an activity on disclosing more personal information than is reasonably necessary to participate in such activity.

[9] "Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section."

a. Do operators take this requirement into account when shaping their online offerings to children?

Not in our experience.

b. Has the prohibition been effective in protecting children's online privacy and safety?

No.

c. Is § 312.7 of the Rule clear and adequate? If not, how could it be improved, consistent with the Act's requirements?

In our opinion, it is not clear or helpful in protecting children. It appears to have the intent to over-ride parental decisions. If parents are willing to consent to the collection of profile information about their child's interests to enable them to participate in an online focus group activity, this provision precludes that by potentially prohibiting the site from making that offer available. When COPPA was first implemented, this was a concern, since few sites had interactive games, activities and prizes. It was assumed that those few could get a child to turnover information in order to access those select offerings. But interactive games, activities and prizes are available on most sites and this concern is no longer relevant.

H. CONFIDENTIALITY, SECURITY AND INTEGRITY OF PERSONAL INFORMATION

26. Section 312.8 of the Rule requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from a child.

a. Have operators implemented sufficient safeguards to protect the confidentiality, security, and integrity of personal information collected from a child?

Rarely. They don't conduct the requisite testing, mapping or management of data to know how secure, confidential or integrity protected the data is. We find problems in most cases even with the most well-intentioned companies.

b. Is § 312.8 of the Rule clear and adequate? If not, how could it be improved, consistent with the Act's requirements?

Providing guidance on what kinds of safeguards are expected, absent a best practices safe harbor, can be helpful.

I. SAFE HARBORS

27. Section 312.10 of the Rule provides that an operator will be deemed in compliance with the Rule's requirements if the operator complies with Commission-approved self- regulatory guidelines (the ''safe harbor'' process).

a. Has the safe harbor process been effective in enhancing compliance with the Rule?

In some cases. Some safe harbor providers are better than others.

b. Should the criteria for Commission approval of a safe harbor program be modified in any way to strengthen the standards currently enumerated in § 312.10(b)?

See below to understand the potential for a safety and best practices safe harbor model that complies with COPPA;s safe harbor requirements while providing more room for innovation and rewards the adoption of best practices.

c. Should § 312.10 be modified to include a requirement that approved safe harbor programs undergo periodic reassessment by the Commission? If so, how often should such assessments be required?

Yes. At least once every 2 years.

d. Should § 312.10(b)(4) of the Rule, regarding the Commission's discretion to initiate an investigation or bring an enforcement action against an operator participating in a safe harbor program, be clarified or modified in any way?

No.

e. Should any other changes be made to the criteria for approval of self- regulatory guidelines, or to the safe harbor process, consistent with the Act's requirements?

Sec. 312.10 Safe harbors provides that:

"(a) In general. An operator will be deemed to be in compliance with the requirements of this part if that operator complies with self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, that, after notice and comment, are approved by the Commission.
(b) Criteria for approval of self-regulatory guidelines. To be approved by the Commission, guidelines must include the following:
(1) A requirement that operators subject to the guidelines (``subject operators'') implement substantially similar requirements that provide the same or greater protections for children as those contained in Secs. 312.2 through 312.9;"

As we examine the best ways to protect children's privacy and keep them safer online, codified best practices enforced by an approved COPPA safe harbor seal holder may be the most effective way to adopt requisite changes to some of COPPA's processes if the safe harbor provides guidelines that are substantially similar to those imposed by the Rule as long as they provide the same or greater protection as those under Secs. 312.2 through 312.9 of the Rule.

At the request of many of our clients, WiredTrust is contemplating the application for a new type of safe harbor seal under COPPA broadening the guidelines to require the use of approved white list, black list and grey list phrase filters and screening practices and moderation technologies. It would require that moderators are vetted and trained, properly supervised, that the risks actually and expected to be encountered by preteens using the operator's site or service are

addressed by policies and processes, and technology systems (if applicable) and that children are taught safe digital technology use and digital literacy, parents are well-informed about the operator's practices and the activities and content used by the operator, as are schools, law enforcement agencies and other policymakers and child protection advocacy groups.

WiredTrust's soon to be announced Socially Safe Best Practices Seal and the Socially Safe Best Practices Kids Seal have already been applied for by many of the leaders of the Internet industry and household family and children's trusted brands. Even without the safe harbor aspects of an approved COPPA seal, the industry leaders have sought WiredTrust's and Parry Aftab's advice on best practices and how to create and maintain safer and more secure networks and digital technologies. Parents will be taught what to look for, and where to come if the Seal participants fail to adhere to the strict guidelines. This new safe harbor standard will help codify best practices and safety in the children's online space. It will certify training, competencies and require in depth reviews of practices, policies and promises made by the Seal participants.

The Socially Safe Seal and Socially Safe Kids Seal are offered by WiredTrust and cover cybersafety and best practices for Web 2.0 sites, interactive digital technologies, tools and features and their related services, games, products and networks (any of the foregoing, a "Community Technology"). The Socially Safe Seal is for a general audience, adult or teen (that are not primarily directed at tweens or preteens) Community Technologies and those that only permit users who are thirteen years of age or older. The Socially Safe Kids Seal is for Community Technologies directed primarily at tweens, preteens and children. Both seals now also cover marketing companies involved in marketing and promotions to children, tweens and teens, technologies and processes approving them for Seal participants.

In order to qualify for the Socially Safe Seal and/or the Socially Safe Kids Seal, an applicant must demonstrate that they already meet, or must adopt and adhere to, best practices for their market segment. This includes adopting and articulating internal operation policies and creating external guides for key stakeholder groups, as specified, for its Community Technologies. It also includes vetting internal staff and outside providers to make sure that risk managers and customer service personnel are selected, trained, supervised and managed in the right way. In addition, they must provide certain information to WiredTrust and updates of that information throughout the term of the Seal.

The Socially Safe best practices guidelines require that the site, network or provider know its users and customers and how their Community Technologies are used. They must understand the stakeholders impacted by their site, network, product or service and identify and address their privacy, safety and communication needs. Socially Safe seal holders must create an internal operation that ensures consistency in customer service and communications. (Too often the safety and security of users depends on which moderator or customer service representative addresses their problem or questions, rather than being a system-wide consistent response.) High risk issues should be handled by risk management personnel trained to address them in the appropriate manner, and escalation policies must be adopted to make sure that reports and problems identified by the network are steered to the right high risk escalation team members. Triaging of reports and identified risks must be built into their moderation and abuse report systems. And data must be maintained for a minimum time to permit responses to be audited and legal access to data for investigations.

Each Socially Safe Seal holder must have a process in place for law enforcement investigations and inquiries and written a guide explaining how that process takes place. They must have addressed the issues of illegal activities and content and created a special communication process for confirmed members of law enforcement who are investigating active cases or who need information regarding the Seal holder's practices, technologies and data retention for official inquiries. The more interactive a Community Technology is, or the more user-generated content (UGC) the Community Technology permits to be shared at the site, the more stringent the standards to address the increased risks.

While the priority is always safety, WiredTrust is practical too. It takes into consideration the size and duration of operation of the Community Technology, as well as its projected risks. (Experts at WiredTrust have been advising the industry, government, law enforcement and the public in these matters since 1995 and can usually forecast risks, as well as identify solutions.)

Start-ups, especially when their user-base is low, have a lower "Threat Profile" by the nature of their size and reduced start-up activity. Once their user-base increases, their obligations to adopt more stringent policies and procedures do as well. Established Community Technologies with smaller adoption rates and those that do not permit UGC or collect location or offline contact information from their users have fewer obligations than their larger counterparts. The Community Technology track record is reviewed as well. Have they been the subject of government regulatory action? Has a COPPA seal program notified them of COPPA violations? Have they had adverse media or attacks from non-profits or user groups? Each of these is evaluated for the purposes of setting the right level of risk-management and best practices standards for each applicant.

Community Technologies directed at children and preteens must be the safest of all, with those directed at teens a close second. Vulnerable demographic groups (such as sexual abuse survivors, cancer patients and special needs groups) and sensitive themes (such as racial or religious topics, abortion and birth control and political debates) are more often targeted online and Community Technologies used by or directed to them must have higher risk management solutions as well. Reports of high-risk activities, such as suicide threats, cutting and self-mutilation, eating disorders and bomb threats, must be handled with the assistance of subject matter experts and specially-trained high-risk moderation staff.

WiredTrust will review the business models, operations, compliance and risks management history and audience of the Seal applicant to help determine the right standards for that Community Technology provider and which levels should apply. Risks are balanced for each applicant in making that determination. Where and how are they operating? How large is their staff? What is the nature of their Community Technology? What is their target demographic? What data do they collect, how and how long is it stored? Is the Community Technology provider an entity with a proven risk management track record, or new to the industry? All of these are reviewed and evaluated and used to help identify the right set of best practice standards that apply to each Community Technology.

This process ensures the integrity of the process and standards but also takes into consideration the challenges faced by small businesses and the scope of risk realities of start-ups and smaller networks. It takes substantial experience and an understanding of how children use technology

and how parents oversee their children's online activities to make this work, but with fifteen years of online safety help group experience and fourteen years of advising the industry leaders and up and coming start-ups in the industry, WiredTrust hopes to be able to help the industry professionalize safety and best practices.

J. STATUTORY REQUIREMENTS

28. Does the commenter propose any modifications to the Rule that may conflict with the statutory provisions of the COPPA Act? For any such proposed modification, does the commenter propose seeking legislative changes to the Act?

    Since 2000 when she testified before Congress on COPPA, Parry Aftab has been proposing that the FTC be given broader powers to set rules and regulations within the spirit of COPPA. She renews that recommendation, knowing that Congressional action at this time is not expected.

PARRY AFTAB BIO

Parry Aftab was one of the first lawyers in the world to practice Internet law. Over the years, she has represented many of the entertainment, Internet and consumer industry trusted brands. Known for her ability to "think outside of the box," she quickly became a leader in the emerging field of Internet law and helped establish best practice standards for the Internet industry. Parry recently founded WiredTrust, a risk management consulting firm, to advise industry and policy makers. While she is an expert in risk management issues for all demographics, a substantial portion of her time is devoted to issues impacting consumer brands, consumers and families online. She is an award-winning columnist for Information Week magazine and 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, brand protection and safety is involved, hers is usually the first name mentioned. Facebook, AOL, Disney, Zynga, Webkinz, Xbox, Build-A-Bear Workshop, MySpace, Liz Claiborne, Hearst, Conde Nast, MTV and Procter & Gamble, 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 second home with her husband in New Brunswick, Canada. She started out on Wall Street 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. Parry founded and continues to run the world's oldest and largest cybersafety and help group, now known as WiredSafety.org as an unpaid volunteer. Dr. Aftab works closely with law enforcement, the Internet industry, educational institutions and governmental agencies, worldwide. Parry Aftab carefully screens all new clients for her consulting firm, WiredTrust. Parry's tagline for industry is "if you're not doing it right, you won't be doing it for long."

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 cyber-marketing and interactive gaming. Because she speaks to thousands of young people and families each month, Dr. Aftab provides a unique perspective and guidance on the design of technologies and marketing practices to address their needs. Since 1994 she has advised the Internet industry on children's and consumer issues. Ten years later, Parry Aftab was the first to develop and promote the adoption of best practices for the Web 2.0 industry. She can spot problems before they occur and help protect trusted brands from online abuse. Unlike other experts, Dr. Aftab's talents include her ability to blend practicality, safety and responsible business practices. 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. Dr. Phil called her a “one-stop-shop” on cybersafety. Jules Polonetsky, AOL’s Chief Privacy Officer, said Parry was “part supermom, part Wonder Woman and part Oprah” 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 US. Parry Aftab was appointed to the Internet Safety Technology Task Force which was identified as a “who’s who of the Internet.” McAfee was the first Chair of McAfee’s consumer advisory board and The Girl Scouts of the USA selected Parry design the cybersafety training for its 2 million Girl Scouts. Parry was appointed to the 24-member Congressionally-mandated NTIA Online Safety Technology Working Group. She is also a member of MTV’s Advisory Board and presents regularly for the FTC on privacy.

Before the

FEDERAL TRADE COMMISSION

Washington, D.C. 20580

In the Matter of:	)	
	)	Docket No. 339
Implementation of the	)	Project No. P104503
Children's Online Privacy Protection Rule	)	16 C.F.R. Part 312

JOINT COMMENTS OF PARRY AFTAB, ESQ., WIREDSAFETY AND WIREDTRUST, INC.

Parry Aftab, in her capacity as a child advocate, Internet privacy and security lawyer and industry advisor, WiredSafety.org, a 501c-3 corporation devoted to Internet and digital safety, privacy and responsible use ("WiredSafety" or "WiredSafety.org") and WiredTrust, Inc., a for-profit risk management and best practices advisory firm ("WiredTrust") respectfully submit these joint comments in response to the Request for Public Comment ("RFC") on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule ("the Rule").

July 12, 2010

Respectfully submitted,

Parry Aftab, Esq.
WiredSafety.org
WiredTrust, Inc.

Parry@Aftab.com
201-670-7250
506-773-5687

WiredSafety operates many programs to empower young users and all stakeholders involved in the safety, wellness, privacy and security of young people. Some are learning resources that can be dovetailed with other programs or dropped into a school day without a large commitment of time or planning. Four are peer-leadership programs creating teen and preteen Internet risk management and responsible use experts, change agents and help groups. We offer train-the-trainers and standard training programs for stakeholder groups such as school resource officers and community police officers, parent s, charities and faith-based organizations. Several programs are tailored to special needs youth (such as deaf and hard-of-hearing students). Many initiatives are designed for parents, caregivers and grandparents to help them navigate the rapidly changing digital environment and learn the benefits of technology. The newer programs address the needs of preschoolers and lapsurfers and students under the age of 8. We have provided a thumbnail description of the top programs, initiatives and resources. The programs number in the hundreds. More information can be provided upon request. All programs are offered without charge, unless pricing is provided in the description of the program, division, initiative, service or resource.

WiredMoms: a combination of a network of volunteer moms and multimedia messaging on digital technology issues appealing to moms. It is an offline and online program, operating as a division of WiredSafety. It hosts events, reviews products, helps moms spot how technology can improve their lives, while helping them protect themselves, their families and the community. It is building a moms' social network and acts as a digital umbrella for other moms groups.

WiredTeens: a new lesson-based program for schools and teens. Described as a "Teenangels lite" it includes 10 lessons, lesson planning materials, resources and guides for teachers and home schooling instructors to use in delivering cybersafety, digital hygiene, information and media literacy, piracy and privacy topics. They cover cyberbullying, sexting, law, mobile technologies, social networking and gaming, as well as passwords, security practices and technologies and helping siblings and younger kids stay safer.

WiredTweens: a new lesson-based program for schools and preteens (8-12). Described as a "Tweenangels lite" it includes 8 lessons, lesson planning materials, resources and guides for teachers and home schooling instructors to use in delivering cybersafety, digital hygiene, information and media literacy, piracy and privacy topics. They cover content issues, cyberbullying, handheld gaming devices, chat, IM, texting, mobile technologies, virtual worlds and MMOGs, as well as passwords, security practices and technologies and netiquette.

WiredKids: a new lesson-based program for schools and students 7 years and younger. It includes 6 lessons, lesson planning materials, resources and guides for teachers and home schooling instructors to use in delivering cybersafety, digital hygiene, information and media literacy and privacy topics. They cover content issues, cyberbullying, handheld gaming devices, chat, IM, texting, mobile technologies, virtual worlds and gaming, as well as passwords, security practices and netiquette.

WiredCops/Cyberlawenforcement: a program for school resource officers, community police officers and law enforcement agencies providing content, resources and help, as well as training in cyber-investigations and emerging issues. Animations, videos, handouts, presentations and guides are provided to law enforcement members allowing them to be used and customized in offline events and on websites. The "WiredCops"

certification program was suspended while being redesigned and will recommence June 2010. Cyberlawenforcement also provided assistance in working law enforcement cases at the request of law enforcement agencies. It is staffed by retired or current law enforcement officer volunteers. New programs are being developed to allow law enforcement agencies to access contact information for law enforcement liaisons at ISPs, SNSs, mobile providers and game sites for active inquiries and investigations.

PeersToPeers: started initially as the copyright and anti-piracy program of WiredSafety, teaching young people to spread the word using the play on P2P, this program will now house the peer-counseling and teen helpline programs offered by WiredSafety teen volunteers and strategic partners. WiredSafety's continuing work and resources will operate under different branding, such as the MPPA Lucky and Flo awareness program for elementary school-aged students.

Teenangels: a teen leadership and expert program enabling 13-18 year old students (and those in college if they had started the program while still in high school) to become advisors to the industry, policymakers, the media and their community. This is a small, but highly effective program, that trains teens as trainers. They conduct presentations to other students, parents, governmental agencies, testify before Congress, serve on brand leaders' advisory boards, consult with online networks and mobile technology providers, help develop messaging and provide help to young people who have been the target of digital abuse. There is a $35 per student cost for shirts and materials which is advanced by WiredSafety. It is repaid through speaking fees and donations generated by the Teenangels chapter. The training, research projects and chapter project typically take between 1 and 2 school years to complete. Advanced programs are in development to enable the students to participate in virtual mentorships and internships with industry and policymakers, worldwide. The training is accomplished in groups or singly, combining offline facilitation, research and observations and Moodle delivered materials and discussions. The training involves 8 large topics with electives. Some topics contain 3 lessons.

Tweenangels: a preteen leadership and expert program enabling 8-12 year old students to contribute their special perspectives in cybersafety and responsible use of digital technology. They focus more on gaming, netiquette, digital hygiene (passwords, malware, etc.) and handheld devices. Digital literacy is an important part of their training as are spotting risks and communicating solutions. They do public speaking and media, typically as a group, and deliver multimedia messages to their peers. Their training combines printable worksheets, animations, computer games, videos and designing programs for their school and community. They too advise the industry and policymakers and appear as experts on TV and offline media. Tweenangels training and research (conducted as a chapter) can easily be completed within one year. The training involves 6 large topics, some of which have 2 lessons.

Sydney Safe Seeker: this program uses serious gaming role-playing and simulation to measure the vulnerability of 5-10 year olds to the ten different categories of sexual predator appeals and ploys used by molesters offline. (The game is being replicated for the online predatorial ploys for a 2011 release.) Identified from Canadian research in child sexual exploitation, these range from appeals for assistance (help me find my puppy," "help me carry this bag" or "point something out on a map for me"), to job offer ploys, curiosity appeals, model and talent agent ploys, threats, authority ploys, confidence and trust appeals, love and affection appeals, gifts and bribes, and fun and games. Children must solve puzzles to earn items that can be used to access different areas of a magical world to find the warpstones which open the portal back to their own world. They are taught the value of

the buddy system and to report “trouble seekers” when they steal something from the gamer’s backpack. The children playing them game are never threatened in the game. The trouble seekers use these same ploys and appeals to trick the children to come closer or go somewhere private with them to allow them to steal an item. The children must identify the physical features, clothing and gender of the troublseeker (using cartoon lineups) to have them captured by the police and their item returned. Every action is measured and tracked and reported to parents, teachers or others supervising their welfare using the accompanying parents application and toolkit. The child’s skills are tracked to show improvement in their vulnerabilities and streetproofing. It is the first of its kind and developed by CSRIC.org, a Canadian strategic partner of WiredSafety. A networked version for schools and law enforcement groups will be available for district wide, schoolwide or classroom use licenses, and a home version for children and their parents/custodians is available for retail download. There is a cost for each.

Alex Wonder Kids Cyberdetective: designed for students between 7-12, Alex combines the aspects of Encyclopedia Brown with the Babysitters Club and Nancy Drew in the digital age. Alex Wonder and his team of cyberdetectives work form the janitor’s closet at their middle school solving cyber-mysteries and problems. They work on cyberbullying, ID theft, cybersecurity and common problems faced by tweens online, in games and with mobile devices and phones. The program uses animated stories, computer games, flash animations, and printables to deliver information and awareness and to help tween become more effective in spotting and addressing risks. This program builds substantial awareness about what can go wrong, how and what bystanders can do to help. It provides information about where and how to report problems to authorities online and offline. Alex debunks misconceptions and helps spread accountable information and resources. This program can be used in the classroom and by homeschoolers to deliver cybersafety education painlessly.

In this computer game, tweens are recruited to join his cyberdetective agency. To earn their credentials, they have to pass the bootcamp challenges and build their handbook. Once they have reached a score of 80% or higher, they are assigned their first cyberbullying case to solve. This is an online game that can be downloaded and played locally. It is sponsored by Microsoft and Candystand.com and is provided without charge. This game will launch in February 2010.

StopCyberbullying: StopCyberbullying.org is an online resource on cyberbullying. It is the most popular cyberbullying prevent website online, according to Google. The site contains information for all stakeholder groups addressing their frequently asked questions and what they need ot know about cyberbullying prevention and what to do if cyberbullying breaks out. The site is being revamped to provide teen help, blogs and multimedia materials for all stakeholder groups.

The StopCyberbullying Toolkit: a downloadable and updateable toolkit being released in February to schools without charge. It contains $850,000 worth of animations, videos, computer games, posters, presentations, guides, printables, content for newsletters, websites and presentations, risk management guides and advisories and projects for students and the community to tackle cyberbullying and sexting. NCPC, the ADL, Michele Borba, Rachel Simmons, Rosalind Wiseman, Build-A-Bear, MTV, Girl Scouts of the USA, AOL, Microsoft, LG Phones, Microsoft, MySpace, Facebook, Spectorsoft, Yahoo!, Proctor & Gamble, the Office of the Mayor of NY, Adobe, myYearbook.com, Disney and others have contributed to this massive resource designed to help schools address all aspects of cyberbullying prevention and risks management, including policies, laws and outreach for guidance counselors, school medical professionals, network administrators, parent/teacher organization, librarians and

library media specialists, school boards and school administrators, educators, technology providers, SROs and safe school professionals. Classroom and extra-curricular activities are provided for K-12, including resources, learning objects and digital media. Yousendit.com and all of our sponsors and strategic partners will help distribute the toolkit to schools online.

The Megan Pledge: designed by a NY chapter of Teenangels and dedicated to Megan Meier's memory, this pledge program involves a printed banner, polka dot ribbons or bracelets, a printed or digital pledge to stop cyberbullying and not see suicide as an option. To date almost 500,000 students have taken the Megan Pledge, which has been featured on TV as well as on myYearbook.com.

The Stop, Block and Tell Program: designed for younger students, for whom the suicide topic may be too overwhelming, this program teaches tweens and younger kids to address all cyberbullying and troubling communications and content they encounter online with three simple steps – stop (don't answer back, print it out or react outwardly), block (the person or the content) and tell (a trusted adult). For younger students there are hand movements to match the steps, as well as a written pledge. Take 5!, an approach that helps them avoid reacting in a harmful way, teaches them to select their favorite offline activity that helps them find balance and to do that for five minutes if something upsets them. They build bulletin boards with their Take 5! Activity and share their favorite activities with others. This program has been adopted by schools worldwide and is the most popular program offered by Wiredsafety to schools and families. Students have written RAP songs, skits and shot videos using this theme. More will be shared online over the next year.

Sumo Pandas: sumo wrestling pandas, including Precious (the wiser one) and Artemus (the constant victim and gullible panda) live and learn in the world of cyberbullying and digital literacy. The pandas often are set off against the polar bears, good and bad. There are short standalone animations, lesson plans designed to use those animations, coloring and worksheets and computer games teaching concepts such as kind words/mean words, too hot and too cold and finding the just right reaction when things go wrong, password selection and security, peer pressure, understanding perspective, the danger of making assumptions, stereotypes and xenophobia. Although students as old as 12-13, it was designed for students between 5 and 11. The full program involves ten animations, several computer games, a Panda "Password Battleship" printable board game, several crossword puzzles and other word puzzles, accompanied by lesson plans, classroom tips and questions and a guide for teachers and homeschoolers.

SuperSafeKiddo: SSK teaches security concepts, such as spyware, pop-ups and password theft. He is a part-human, part computer super hero who attended super hero correspondence school and didn't study very hard. While he is inept, his sidekick "Bot" isn't. Students learn through slapstick animations featuring SSK and Bot. This program and theme was designed for students 7-12. The classroom materials to support more learning using this character line are being prepared and will be available for school year 2010-11. The line of existing materials includes posters, coloring sheets, worksheets and several animations.

Take Back the Net: a multi-stakeholder initiative involving media, schools, community and advocacy groups, law enforcement, seniors, families, businesses, college students and adults and the technology industry itself. In a series of offline events which work hand-in-hand with a huge takebackthenet.com portal testing their safety and security IQ, vulnerabilities and cyber-practices.

LMK.GirlScouts.org: created by Parry Aftab for the Girl Scouts of the USA as their cybersafety change-agent project, the LMK website takes the standard and boring cybersafety messaging and makes it relevant for teens. Instead of lecturing them, it addresses their questions. It puts them in a leadership role in helping create a safer digital experience for themselves and their friends. A monthly newsletter written by the teen board and guided by Parry helps deliver the Girl Scout message to parents. The Girls Scouts has more than 2.5 million girls.

A Thin Line: designed by the public affairs team at MTV Networks, this campaign takes cybersafety and makes it cool. Understanding that teens didn't respond to the term "cyberbullying," they changed the vocabulary to "digital abuse." Using award-winning directors and the creative talents of MTV, combined with an advisory board comprised of the leading experts in teen dating abuse, harassment and digital abuse (including Parry Aftab and Casi Lumbra, one of the Teenangels), this multi-year and media campaign will give young adults a place to go for help, information and to find ways to change things for the better. A video contest has been launched to get teens to design a documentary/video. Following in the footsteps of Rock the Vote, athinline.org should change the landscape. Wiredsafety contributed significantly to the content and structure of the program.

Love is Not Abuse: an award-winning program created by Liz Claiborne to address dating abuse issues. WiredSafety developed the digital dating abuse materials for their curriculum, launching in February 2010.

Don't Be Stupid: a teen inspired message to other teens and preteens about sexting and high risk activities online. It communicates the risks teens and preteens take needlessly and willingly online. This campaign is particularly effective with high risk youth who are rarely responsive to more traditional messaging.

ThinkB4uClick: using handouts, quizzes and interactive, this program teaches teens about avoiding common problems encountered when they don't check the recipient's address, don't bother to read something over before sending or let off steam online. Practical information, step-by-step approaches and easy tips help them avoid sending the message to the wrong person, leaving out a "not" or playing a practical joke that isn't seen as a joke online. It's about digital literacy and hygiene.

Internet Safety through Information Literacy: created by WiredSafety's technology education division head, Art Wolinsky, this program merges cybersafety into the larger topic of information literacy. It teaches students how to judge reliable and hyped content, protect their identities and data, understand the concept of privacy and be good cybercitizens. It uses a series of learning objects and short resources that can be easily dropped into a class period to help deliver learning in a more flexible style. It has been used by teachers across the US and worldwide.

Digital Hygiene: this program teaches all stakeholders about password and login risk management, security software, how to use public and shared-use computers securely, commonly-exploited devices and methods of exploitation (lifting and reprogramming a cell phone when it is unattended) and ways to avoid becoming victimized online through the use of easy digital risk management techniques. The messaging is delivered online, offline and using multi-media, in each case using examples and content geared to that target demographic group.

The Kids Internet Bill of Rights: this campaign teaches 8-12 year olds about their online legal rights and obligations, and helps them learn how to insist that their privacy be respected, they are free of unsolicited emails and IMs, they don't have to view "creepy" or "gross" content and have their friends not access their accounts without permission. It is an affirmative message, reminding them that they have rights and should let others

know that they want those rights protected. The uppermost message is that “I have the right to use the Internet without others hurting me, being mean to me or making me see things I don’t want to see.”

Sextbullying: a new site to be launched under the stopcyberbullying banner, this addresses sexting abuse and shares the sad truth about how your classmates can use your private sext as a weapon to hurt you. It also discusses the current state of the child pornography and online harassment laws in the US and Canada.

What Were You Thinking?: designed to address reputational risks, this program uses videos produced by teens and young adults to share the message that “what you post online stays online…forever!” It discusses consequences and how even a “friends only” setting doesn’t mean you are protected.

Have the Talk: a website in production that helps young people and their families and friends understand how to have the tough conversations about cyberabuse and safety. It will include scripting of a typical conversation on different hard topics as well as features that permit a parent, family member of young person to send a template message to someone they care about to make it easier to get the conversation started. This will address situations when a private sexting image works its way to the public and a teen needs to tell their parents, when friends feel offended by something their BFF did online that hurt them and parents having problems expressing their concerns. Eventually this will include suggested conversations for other family-related risks and tough topics working with other NGOs.

The StopCyberbullying Coalition: made up of the leading online and offline brands and other advocacy groups and experts dedicated to stopping cyberbullying. They are committed to sharing expertise and resources and working together to improve practices and change thing for the better. It was founded by and is run by WiredSafety.

Netiquette: many cyber-risks can be avoided if we just took a minute to think about the person on the other side and treated them and ourselves with more respect. Students K-6 are given a template and guidance to create their own netiquette guide or can modify Ms. Parry’s Guide to Good Manners Online, a tongue in cheek netiquette guide. They can share their guide, print it out or submit it for publication on WiredKids.org.

WiredSafety Speaker Program: to address the increased demand for knowledgeable and entertaining speakers across the US and Canada WiredSafety trains its volunteers and professional speakers to deliver presentations using its resources and expertise. There is a charge for these presentations. Sometimes donations are made to Wiredsafety as well. Teenangels provide presentations locally for a $400 donation to their chapter’s work. A WiredSafety certified speaker program is in development, certifying those who have proven their expertise and proficiency in educating their audience.

MPAA’s Lucky and Flo Anti-Piracy Awareness: developed with the MPAA using their CD and DVD-sniffing Labrador retriever service dogs, this program helps elementary school students understand the high cost of counterfeit and pirated movies and videos. Weekly Reader has developed a curriculum to accompany the Lucky and Flo awareness program.

“WiredSafety Partners” Programs: together with Cisco, Liz Claiborne, MTV, Nickelodeon, Disney, Microsoft, Xbox, Webkinz, Build-A-Bear, Runescape, AOL, Seventeen Magazine, Proctor & Gamble, Hearst, Conde Nast, CMP, KidZui, Facebook, Children’s Television Workshop, Zynga, CTIA, Verizon, LG and others, Wiredsafety has created

cybersafety messaging that addresses the needs of the brand name audiences. It is the trusted partner for every major campaign on cybersafety.

Wired Kids Summits, WiredSafety Events and Briefings: for more than eleven years Wiredsafety has been hosting events to bring the latest information and trends to the public, industry leaders and policymakers worldwide. The StopCyberbullying Summit in June 2008 was streamed internationally and viewed by more than 100,000 people around the world. Verizon's Chairman and CEO, Ivan Seidenberg, was the event's luncheon speaker. Its WiredKids Summit, in its 11th year, is given annually on Capitol Hill and is run entirely by Teenangels and Tweenangels. The room is always packed, seeking the latest research conducted by the teens and tweens.

WiredSafety Outreach: providing content for all stakeholders' cybersafety and best practices needs that can be used on other sites, printed out and distributed and used on profiles and in viral campaigns, this provides expert and entertaining content that all cybercitizens can use and share.

WiredSafety's Best Practices: having worked in the field for 14 years, advised leaders and start-ups in the industry and handled cyberabuse reports when things go wrong, WiredSafety knows what enterprises need to do to do it right. The new SociallySafe Seal and the Socially Safe Kids Seal have adopted these strenuous best practices standards.

TESTIMONY OF

PARRY AFTAB, ESQ.

(THE KIDS INTERNET LAWYER)

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON COMMERCE, SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

OCTOBER 11, 2000, 10:00 A.M.
RAYBURN HOUSE OFFICE BUILDING, ROOM 2123

Parry Aftab, Esq.
Special Counsel
Darby & Darby, P.C.
(Intellectual Property and New Media Law)
805 Third Avenue
New York, New York 10022
www.darbylaw.com
Phone: (212) 527-7751
Fax: (212) 753-6237

Email:parry@aftab.com
www.aftab.com

TABLE OF CONTENTS

Summary

The children's Internet industry is facing tough times with finding a viable and consistent revenue model, getting parents involved with what their children are doing online, keeping children (and investors) happy, and navigating the regulatory waters.

It's important that we understand that this is a complicated combination of factors, and no one is to blame. Coincidently COPPA came into effect shortly following the falloff of Internet stocks and venture capitalist interest and because of this, COPPA and the FTC are being unfairly blamed for problems being encountered by the children's Internet industry generally.

That doesn't mean that COPPA couldn't be fixed to provide solutions to the real problems encountered by children online, such as unethical marketing practices, the collection of their personal information, and online predators, in a more industry-friendly way. The best way to do that is to provide the FTC with more discretion, rather than less. This would encourage sites to become safer and guard their children visitors' privacy more carefully, in exchange for reduced regulatory obligations. It would allow the FTC to tailor compliance requirements to the sites' use of personal information from children and level of safety measures used in designing interactive features. (That means the FTC would be able to approve certain chat programs, if they use moderators to supervise the children's chat activities and use technology designed to screen out children's use of real identities online in open chatrooms.) This would allow sites who actually cared about children's safety and privacy to be more innovative, and be rewarded with not having to obtain full-fledged verifiable parental consent.

Solutions need to come from Congress, the FTC and the industry itself. And parents' and children's interest use and concerns need to be studied to make all the solutions more effective and relevant. The last thing we need to recognize is that teaching children safe surfing practices and teaching parents how to understand what their children are doing online is the real answer. Education is far more important in this field than more regulation.

Snapshot of The Children's Internet Industry

There is no more exciting or rewarding industry than the children's Internet industry. Where else can you have fun, help children and change the world at the same time? When you deal with children, safety, quality content and privacy are good business. Parents are partners in this. But, as exciting and potentially rewarding as it is, the children's Internet industry is facing many challenges, these days, and they need help from both within the industry and from regulators, in order to face those challenges and make sure that what's best for children is always foremost.

Who are the players?
The children's Internet industry is largely dominated by U.S. sites. They typically fall into three categories, (i) large, well-recognized leaders in children's entertainment and media, such as Disney (disney.com), Viacom (Nickelodeon, nick.com, and nickjr.com, and MTV, mtv.com), Fox, PBS (pbs.org/kids), Sesame Workshop (the new name for Children's Television Workshop – Sesame Street, sesamestreet.org), Sports Illustrated (sikids.com), Nintendo (nintendo.com), and Cartoon Network (cartoonnetwork.com), (ii) new players to children's media, which came from the Internet, as opposed to traditional entertainment media, such as Surfmonkey (surfmonkey.com), MaMaMedia (mamamedia.com), Freezone (freezone.com)), Bonus (bonus.com), Alfy (alfy.com and cleverisland.com), Zeeks (zeeks.com), Lycoszone (Lycos's kids site, lycoszone.com), Yahooligans (Yahoo's kids site, yahooligans.com) and, until recently, Headbone (headbone.com), and (iii) sites that are linked to educational services, media and products, such as Chancery Software (k12planet.com), Discovery Channel (discoverykids.com), Scholastic (scholastic.com), Weekly Reader (weeklyreader.com), National Geographic (nationalgeographic.com/kids), Princeton Review (homeroom.com), Big Chalk (bigchalk.com and homeworkcentral.com) and ePALS (epals.com, a penpal service for schools using e-mail rather than traditional postal mail).

How do they operate?
Generally the children's Internet industry operates on a B to C business model. That means they are businesses delivering services to consumers. Essentially they offer kids content, games and interactivity to children. Most sites are free. Some sites require that children register to be able to access certain content and services. That registration may require personally identifiable information and therefore parental consent under the new children's online privacy law, The Children's Online Privacy Protection Act ("COPPA," described later in this testimony and the appendix), but many only require that a child inputs a user name (using anything they want) and password. Some sites operate on a subscription model, charging parents, sponsors and in some cases even parents' employers (see Kids Online America, kola.net), for subscriptions to special services and content for children.

But B to C models have fallen into disfavor with the venture capitalists, recently. Therefore, some children's Internet industry members have recently changed their model (or gone back to their original models) to a B to B model, offering their services to other businesses, even within the children's Internet industry itself. Most notable among these is, perhaps, Surfmonkey (surfmonkey.com) which started out as a technology company, specializing in browser technology and content management. When the market (and venture capitalists) cried out for portals, it repositioned itself as a children's portal, providing content, branded media and interactive features to children. It's now designing a special browser that provides content management to preapproved content, allowing parents to select content filters, and manage their children's access to chatrooms, instant messaging, e-mail and other interactive tools and even their time online. This is being offered to other children's sites to allow them to have interactive communities, without having to jump through the regulatory hoops.

The Children's Internet Industry is facing difficult times.

Last month, there was an industry-wide conference for members of the children's Internet industry. A representative of one well-known children's site commented to a panel (that included me) on COPPA compliance in the kids Internet industry. This woman stated that if you are involved in the kids space, your primary obligation is safety and privacy. She said that all children's sites need to be obsessed with safety and privacy of their site visitors. A representative of another well-known children's site stood up, and said although they cared deeply about online safety and privacy for children, they were "obsessed" with the bottom line.

I have never heard a comment repeated within the industry as often as this response. That's because it spoke to the hearts of all members of the children's Internet industry. While most of the industry is focused on online safety and

privacy and doing what's right for children, many have forgotten to stay focused on staying in business. There are several solutions for this, and no one area to blame. One essential solution is to educate sites on business models and help them work with others to stay successful. In response to this, we are forming the first children's Internet industry trade association, to operate in alliance with an existing umbrella non-profit dedicated to children's equitable access, education online resources and safety and privacy issues, WiredKids.org. This organization is creating KITA, the Kids Internet Trade Association, to help sites address these issues, learn what they need to know to keep their businesses operating and help them network with others within the industry and government on these issues. It will include filtering companies, ISPs, technology companies, educational services, content providers, media providers and others involved either directly or indirectly with this industry. But although a help to the sites, this will not address all of the issues faced by the industry.

Problems faced by the Children's Internet Industry:
While children are online more and more (roughly 25 million in the U.S. alone under the age of 18), few children's sites have been able to find a single business and revenue model that works in the kids space. (Children's sites for the purposes hereof are directed at children and preteens.) While children may be loyal site visitors, parents aren't supporting the industry in sufficient numbers. The key to success of the children's Internet industry is to get parents to understand the value of their children's online activities, and support them.

Most sites in the kids space are using a combination of several revenue models that are helping them stay afloat until parents find a compelling reason to support the children's Internet industry. (This will come over the next few years with the delivery of educational services, games, videos, online music delivery and new media and programmable toys that can only be programmed online.) When we can find the model that parents find compelling, the kids space will be very successful. But during this interim period, between the earlier excitement over the children's Internet industry and finding the right revenue model and what parents find compelling, the industry is facing hard and lean times.

This makes the industry particularly vulnerable to other factors and outside influences. Prime among outside factors are: tech and Internet stocks are down, the IPO market for the Internet industry has slowed, and the venture capitalist money in the Internet space has been drying up or directed at currently profitable e-ventures, generally, Many sites that were planning on rounds of financing after February, 2000, found themselves without funding because of the market downturn last Spring. Several proposed mergers and combinations that involved some of the kids space leaders fell through, causing these sites to waste months and even years in discussions. Time that would have been better spent, in hindsight, developing revenue models and maintaining their dominance in the space.

In addition, being involved in kids content development and delivery is very costly and particularly time intensive for sites other than Disney, Fox, Nickelodeon and the like, whose business is the development of content online and offline for children. Couple this with the high cost of maintaining a safe site for children (with moderators in chatrooms and oversight of what the children are doing and posting at the site), confusion over the years as to what the market needed (largely driven by the venture capitalists) and the speedbumps caused by regulations make it very difficult and costly to operate a children's site and it's no wonder many are struggling to stay afloat. Some wonderful sites have already lost and are losing that battle.

While many are now blaming the FTC and COPPA, however, this isn't fair and isn't a true reflection of the situation. It is a complicated combination of factors that is making the life of a children's Internet site precarious. Since many of these factors came to bear after the March downturn in the market, and COPPA came into effect in April, COPPA is an easy target for blame. But there is no *one* culprit here. And if there is, it isn't COPPA. COPPA plays a role in the problem, but more as a result of parental lassitude and in the lack of flexibility and discretion given to the FTC to administer COPPA and provide carveouts for other safe models.

There are seven issues that are creating special challenges for the industry: (i) no clear revenue model has been generally identified as working for the kids Internet industry, (ii) parents say they care about children's online safety and privacy, but aren't taking the time and effort to do anything about it and are unwilling to pay for most online content, (iii) the venture capitalists, angel funding and public security markets have become more cautious since the Spring 2000 downturn of the Internet markets, (iv) content development is very costly and time-consuming, (v) children are not candidates at this time for viable e-commerce and direct purchasing online, (vi) parents are often unwilling to use credit cards and other adult verifiers online, without a compelling reason to do so, and (vii)

regulations pose difficulties when preteen-interactivity is involved, which decreases traffic, which further decreases the likelihood of obtaining financing. Each of these points, either individually or in combination with one or more of the other points, is examined below.

No generally identified business and revenue model exists yet for the children's Internet industry:

Currently the children's Internet industry is struggling to discover a viable generally-applicable business model for supporting children's content and features online. At this time, most are using a combination of revenue models to support the high cost of maintaining entertaining and fresh content for children and preteens. Some good sites, which children enjoyed and parents approved of, have been unable to survive during this difficult time for the children's Internet industry. Even the ones that have survived the downturn on e-commerce and Internet investments, the falloff of the IPO markets, the high costs of safety and privacy safeguards and legal compliance, and the lack of parental enthusiasm and support, are struggling to find a viable and consistent business and revenue model.

Advertising:
Advertising, while a portion of most site's business models, isn't able to support the costs of maintaining children's online content. Advertisers are currently seeking a new interactive model for Internet-based advertising that may be more effective with children, but the advertising typically used (click-thru banners) isn't producing the results advertisers are seeking. This will, hopefully change. Children, while capable of influencing offline and online purchases, are not yet participating in e-commerce. This both affects the advertising rates and the ways in which advertisers are willing to work with children's sites.

E-Commerce:
Children, for the most part, don't purchase products online. They research products and services, but are not purchasing them online. Teens are starting to become an e-commerce force online, but this has not extended to children and preteens. Children and preteens influence offline spending of their parents in large amounts, however. While a few kids e-commerce sites exist (relying largely on the gift registry and gift certificate concept, such as iCanBuy.com, RocketCash.com and doughNET.com), this isn't generally a standalone viable business model at this time for the children's Internet industry, either. E-commerce for children isn't compelling enough yet for parents to support in large enough numbers. This will change over the next few years when services and products that children want most are only available online (such as programmable toys, computer games and, to serve the desires of parents, educational services; for an example, see Homeroom.com, offered by Princeton Review).

Sponsorship:
Sponsorship is a business model used by many children's websites during the last few years. Some use it to handle the costs of a particular feature or section of their own site. Others use it to design sites for other companies. Some large brick and mortar, offline corporations have paid for the development of special sites directed at children. Fleet Kids (designed by Headbone, one of the saddest casualties of the children's Internet industry) is a notable example of how the offline industry can join forces with the children's Internet industry to develop educational and entertaining resources for children. But, the revenues raised through sponsorships are generally insufficient to defray the costs of running an entire children's site. Some notable specialists in the area of kids website designs for other companies are Media Jelly, which designed the Magic School Bus site for Scholastic and Goosebumps, among other award winning sites (www.mediajelly.com), and Zeeks (formerly a popular child portal and now using their expertise to create sites for others).

Marketing and Collecting Data:
One model many general audience sites use is collecting marketing and demographic information about site users. They may have site registrants provide personal information, such as income, occupation, educational levels, addresses, telephone numbers and e-mail addresses and pair this with their surfing practices, marketing preferences and buying practices. Many members of the children's Internet industry had been collecting personally identifiable information from children at their site. When parents learned about this, they reacted strongly. This is one of the abuses COPPA was designed to prevent.

But marketing and demographic aggregate information not tied to a specific child could be a partial business model for popular sites. While children's sites could easy collect and aggregate non-personally identifiable information and

still be in compliance with the law, most either don't know how to do this, or haven't discovered the value of sharing their expertise about children's preferences with marketers, in aggregate demographic mode. For example, Nike wouldn't need to know that Billy Smith from 100 Main Street in Englewood, N.J. who attends fourth grade at the Englewood Grammar School likes blue sneakers more than black ones. They need to know that fourth grade boys in the NY metropolitan area prefer blue sneakers to black ones. This lets them market to all fourth grade boys, rather than directing ads to Billy via his e-mail or by directing special ads to him when he surfs online. This isn't as valuable to advertisers that may be seeking direct marketing opportunities, but it may help increase revenues. And here, COPPA levels the playing field between those sites willing to collect and mine personally identifiable data from children, and those that refuse to use their young site visitors in that way. With advertisers limited in what can be collected and shared without verifiable parental consent, the sites find it easier to direct them to aggregate demographic information options.

Subscription-Based Models:
The subscription model hasn't been successful to date. Parents are unwilling, generally, to pay for children's online content. Some new sites will be offering special features and content, which may hopefully change this. Alfy, one of the leading kids content Internet sites is launching its new subscription-based model, cleverisland.com. Disney is focusing again on its Disney Club Blast! (disneyblast.com) subscription site (the site has been in existence for several years and is now entirely made-over). This has the additional parental attraction (and therefore, potential for success) of being Disney content. Juniornet (juniornet.com) has been a subscription-based service since its launch in 1997, and was the first of the new types of closed access services, which provide selected Internet content within a "walled garden" rather than from the Internet itself.

The experts see the subscription model as one of the most hopeful for the children's Internet industry, at least until software, games and educational services are regularly delivered online (about two to three years down the road) and parents are forced through market pressure to pay attention to their children's online activities.

Parental Involvement*:*
Parents care about privacy and online safety, but they aren't interacting with the sites or supporting the sites that protect their children's safety and privacy. It may be that they are intimidated, or just plain too busy. But the children's online laws depend on obtaining parental consent, and if parents aren't bothering to provide consent, sites are running into problems.

Bonus's experience is a case in point. It found that out of the parents who were asked for their consent for Bonus to use children's information internally, 51% never replied, 31% provided consent and 5% said "no." (13% are still pending from this sample group.) This was a six to one ratio of parents allowing their children to use those services, over those who wouldn't allow them to share the information. But the 51% of parents not bothering to respond is frightening.

Bonus is losing more than half of the children who want to participate. And Bonus doesn't have chat, e-mail, e-commerce, on instant messaging. Bonus is a site that has games for children, and sends newsletters to their site visitors. This is a typical situation faced by many children's sites.

The solution is two-fold. One we need to teach parents how important they are to their children's safe and private online experience. They often feel that since their children understand the technology, they don't have to get involved. But they need to recognize that, although their children's technological skills may exceed their own, their children haven't yet developed the requisite judgment for handling communications with strangers online safely, at a younger age. Kids have better tech skills, but parents have better judgment.

We need them to understand the real risks children face online. Parents need to see the Internet as the telephone, rather than the television. While they may be concerned about too much sex and violence on television, parents are rarely compelled to take action in connection with what their children see on TV. Yet, all parents feel compelled to make sure our children do not talk to strangers. None of us would allow our child to talk on the phone with an adult stranger for two hours. Yet, their children often do just that, online in chatrooms and using instant messaging. Once we can get parents to see their children's safety and privacy in terms they understand, such as the telephone calls with stranger, they can use common sense to help their children learn how to surf safely. (Detailed information on all aspects of online safety for children can be found in my new book, The Parent's Guide to Protecting Your

Children in Cyberspace, McGraw-Hill, 2000 (retail price $12.95), copies of which will be provided to the Subcommittee.)

Two, we need to make it easy for parents. If they need to provide consent to ten sites their children visit, separately, they just won't do it. We have worked on this issue as well, by developing a central site registry where parents can make a donation to Wired Kids via credit card, and register at one time for as many member sites as they want. A second service for parents is being developed with Wired Kids, where parents give noted online safety experts the right to approve sites for their children, based on certain criteria set by the parents, such as moderated chatrooms.

But these are a drop in the bucket, and more intensive parental consent mechanisms need to be developed. Offline consent, obtained at certain store locations from parents may be one possible solution. Parents who are shopping at a store may be able to use an offline consent gathered there to give the level of consent for their children's online interactivity. Schools are another place to collect consents.

Schools are being used by large sites for parental collection systems already. Big Chalk works with more than 26 million children in more than 42,000 schools. Chancery Software (k12planet.com) works with 20 million children in US schools. Under existing regulations and guidelines, sites are permitted to rely on the school's representation that the parents have consented to the student providing the personally identifiable information or using interactive features at the site. If schools make this representation, the site has millions of registered children and has complied with COPPA without having to deal directly with the parent. This is creating a risk management issue for schools, however, which may or may not have actually obtained the parents' verifiable consent.

Sources of Funding and Financing:

Venture capitalists have pulled back from the children's Internet industry. A couple years ago, venture capitalists first became interested in the children's Internet industry. Until then, their main focus had been in e-commerce, but as more and more children got online (with a growth from 6 million in 1996 to more than 25 million today in the United States alone), the children's portion of the industry became more attractive. But the venture capitalists were looking for potential IPOs, and the IPO market has been dry for most of the Internet industry. Without IPO potential, and with no presently viable generally-recognized business model, venture capital dried up, and the chance for many children's sites to survive largely dried up with it.

Many sites had periodic financing schedules. Those that managed to raise their financing prior to the market correction this past spring are sitting pretty in the kids space. Others have international investment and business and revenue models. This too gives them more flexibility. But many found their expectations of being able to raise the financing they needed, as they always had raised them, unrealistic. Depending on how long they had waited in the financing cycle, many found themselves unable to keep their doors open. Most cut staff, changed operations and looked to other avenues for revenue. Licensing content and strategic alliances were seen as potential new revenue models, and have helped several sites survive and have brought others a higher profile outside of the traditional kids space. Brick and mortar children's industry players became more important and educational resources, which had additional value to bring to the mix, became more prominent.

Kids Online Privacy, the FTC and COPPA:

While there is a substantial focus on COPPA today, and the costs of compliance and to the industry, it is also important that we remember why COPPA was passed in the first place, and the serious risks to children is was intended to address.

COPPA was intended to address two separate concerns, (i) over-marketing to children and collection of personally identifiable information from children that is shared with advertisers and marketers, and (ii) children sharing information with online predators who could use it to find them offline. Both are valid concerns and need to be addressed.

Children's Online Marketing Practices:

The FTC has conducted several surveys of websites, both sites directed at children and general audience sites. In each survey they learned that sites were collecting personal information from children, not informing the site visitors about their information collection practices and what they did with the information collected, and in many cases sharing this information with marketers and advertisers. While the bulk of the credible online community took this issue very seriously and drafted clear privacy policies and instituted ethical collection practices when children were involved, far too many sites ignored the FTC's warnings and plea for self-regulation from the children's Internet industry itself.

Interestingly enough, the practice of collecting and sharing personally identifiable information about children has been almost entirely eradicated. No credible children's site is currently collecting personal information from children for outside marketing, and none are knowingly sharing information collected with third parties. So COPPA works in this respect. It has changed an industry practice – one that parents wanted changed.

A sunset provision has been adopted and is in effect until April, 2002, that allows sites to collect personally identifiable information from children (this includes e-mail addresses, as well as what we would normally consider personally identifiable information) for internal use only with less than full-fledged "verifiable parental consent" (which is currently, typically, via telephone, credit card or debit card verifiers, regular postal mail or fax). During the sunset period, parents can provide their consent via e-mail, provided that the e-mail requesting this consent is delivered in such a way as to make it more likely that the parent and not the child will receive the e-mail and provide consent, and providing that the email consent is confirmed in some way. This is an "opt in" model that only permits the child's information to remain on file and be used if the parents affirmatively consent to it, by replying to the notice. As discussed in more detail later, we describe the actual statistics obtained from a leading children's site, Bonus. Bonus reports that more than 51% of the parents don't bother to respond to this e-mail. Of those who do respond, there is a six to one ratio of those providing consent, as opposed to refusing it.

Protecting Children from Online Predators:
The second concern intended to be addressed by COPPA was children being lured and stalked by online predators who gather information about them from chatrooms, instant messaging, e-mails, websites and the like.

This is a very real risk, and one that should be addressed. Last year the FBI's Innocent Images Unit (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 experience, about the same number of cases were opened by state and local law enforcement agencies last year for the same crime. Out of 25 million underage Internet users from the U.S., 3,000 cases may not seem like very much (especially when often it is a law enforcement agent posing as a child who is being lured, not a real child victim), but one if too much and all of these cases are currently avoidable. Also, most child molesters have a history of abusing children, so each case represents harm done to more than one child. 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. Teen People has an article I worked on with them, on this very issue, in its new November issue, now out on the stands.

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.

COPPA in Practice

Parents have told me that having to provide verifiable consent is a burden, although they are grateful that someone is notifying them of their children's online activities. They are also complaining that their children cannot use the interactive tools immediately upon obtaining their consent, given the current process which is largely offline. They object to using their credit card information, and credit card companies are unhappy that their verification systems are being used for this purpose. The charge to a site for credit card verification, for these purposes, is $.10 to $.20

per verification (generally per child). Sites are also being pressured not to use the merchant account systems for this purpose.

Obviously, the issues that COPPA was designed to address are still of great importance. But many of the problems cited in connection with COPPA could be handled easily if the FTC had more discretion in approving exceptions to full verifiable parental consent for safe applications and site practices. The law, as finally adopted, gave the FTC little or no discretion in this regard. It is the lack of flexibility, rather than the law itself, which presents the greatest problem.

While COPPA has received much criticism from members of the children's Internet industry, whether or not it is warranted, the FTC deserves only praise. The FTC has been outstanding in trying to inform the industry of what COPPA provides and how to comply with COPPA. They have been available for private meetings with site operators, have held a clinic on COPPA and how to comply, and have been active speaking at industry conferences on the law and how it affects the children's industry and general audience sites.

Cost of COPPA-compliance:

We have polled most of the mid-sized children's websites for the cost of COPPA-compliance, in hard dollars, not as to any lost revenue or loss in traffic. This can run from more than $115,000 per year to $290,000 per year, depending on whether the site is fully interactive, with chatrooms, etc. and what level of consent they collect. Here's what they told us:

- $10,000 - 15,000 for legal, including audits and construction of privacy practices and policy
- Cost of toll-free telephone and dedicated fax service
- $35,000 in engineering costs to make the site complaint
- $2,500 - $10,000 monthly for professional chat moderators (price differs depending on training, hours of operation and organization)
- $35-60,000 per year for one person to oversee offline consent, respond to parents= questions, review phone consents, and review permission forms.
- $35-60,000 per year for person to oversee compliance, database security, respond to verification and access requests.

One specific example of a site and how it is dealing with COPPA is ePALS.

ePALS Classroom Exchange™ is the world's largest online classroom community and the leading provider of collaborative classroom technology. ePALS pioneered the collaborative classroom concept in 1996 and now connects more than 2.5 million students and teachers in 182 countries worldwide.

ePALS Community members use a set of free, collaborative tools to meet and correspond online, combine professional expertise, join interactive projects, and develop international friendships. This tool set includes extensive profile creation and search functions, monitored email with profanity filters, moderated discussion boards, private chat, and soon, photo sharing technology. ePALS works to balance participation in the global community and learning through collaboration against the safety concerns of our educational community.

Educators turn to ePALS for a safe, creative way to integrate technology into the curriculum and to introduce students to the skills they'll need to participate in the global community. The ePALS commitment to safety is an ongoing success story.

ePALS has developed a simple COPPA consent package for American teachers who are already registered with ePALS. Teachers download this package directly from www.epals.com, print it and distribute consent forms to their students to take home to their parents. Only when all the consent forms have been received is the teacher free to carry on with ePALS activities. For all new teacher registrations, ePALS requires teachers to collect consent forms before they can set up monitored email accounts for their students.

All individuals registering with ePALS must now submit their birth date and citizenship. If the individual is under 13 and from the United States, the registration process requests the parent's email address to complete the sign-up. Without the email address, the registration cannot be completed. If the child does provide his/her parent's email address, ePALS sends the parent a copy of the ePALS privacy policy (http://www.epals.com/privacy/index_en.html) and a consent form, which must be signed and returned via fax or post. Parents may also use a special toll-free number to provide their consent. ePALS will not activate a child's account without verifiable parental consent.

Beyond securing parental consent, the ePALS site offers three additional layers of security:

1) All profiles submitted to ePALS must be read and approved by a trained Site Support Coordinator before they are added to the site. Suspicious profiles are refused immediately.

2) The profile creator, the teacher or parent, is the first point of contact for anyone interested in a class/group profile. The teacher or parent can decide to refuse any communication.

The teacher or parent has comprehensive access to ongoing communications for his/her group of children. He/She can read every incoming and outgoing piece of email before it is received or sent, or simply choose to read specified pieces -- ones with attachments, profanity, etc. The choice is up to the teacher or parent.

An example of what had to be undertaken to make ePALS COPPA-compliant:

- Massive revision of registration system to capture age, nationality, and parent/guardian information, send data to parent/guardian, and restrict access to appropriate users
- Revisions of Privacy Policy
- Creation of COPPA consent forms
- Installation of dedicated phone and fax system
- Hiring and training of Site Support staff to administer COPPA consent process
- Ongoing legal counsel
- Teachers cannot use ePALS in their classrooms until parental consent is received

Potential Solutions in Connection with COPPA

As discussed in more detail at the end of this section, solutions will come from three areas.

First is from Congress itself:

- We need studies conducted about how children use the Internet, and what help parents want and need.
- We also need funding for Internet safety education in schools and community groups.
- We need governmental support of leading Internet safety advocates t help them do their job in educating parents and children, and providing helplines for those who run into trouble online.
- We need more funding for law enforcement, to fight crimes against children online.
- We need more training of state and local law enforcement agencies to help fight crimes against children online.
- We need more discretion given to the FTC, and practical and reasonable carevouts from COPPA, or reduced consent levels, for sites that can demonstrate that they care about children's privacy and online safety.
- The FTC needs more funding to hire and retain quality staff experienced in this field. (The FTC staff is stretched too thin, and its staff members are too often recruited and hired by Internet industry members who need experienced advisors.)

Second is from the FTC itself, many of which are already implemented:

- We need more education of the industry in how COPPA works, and how sites can comply. (The FTC held an unprecedented clinic on compliance in August, and has been outstandingly proactive in this area.)
- We need a close interaction between the industry and the FTC in the area of online safety and privacy, and new technologies. (Here, too, the FTC deserves praise for its accessibility to the industry and its willingness to keep open dialogue with members of the children's Internet industry, large and small.)
- We need more FTC staff in the area of privacy and Internet consumer protection issues.
- Once more discretion is given to the FTC, we need it to address other methods of protecting children's safety and privacy under COPPA, which may allow sites to avoid the offline consent mechanisms.
- We need help in educating parents and children about online safety and privacy.

Third is from the industry:

- We need to work together to form solutions, such a central registries, and joint consent mechanisms, and consent mechanisms where parents set the standards and allow a trusted third party to select the sites which satisfy the guidelines approved by the parents.
- We need to educate the children's Internet industry on business and revenue models and provide them with skills they need to run their businesses profitably. (The new trade association will help address that.)
- We need to educate parents about online safety and privacy, and educate children on safe surfing practices and how to exercise critical thinking online.
- We need to develop new technologies that make Internet safety and privacy as seamless as offline safety and privacy.
- We need to share our concerns and recognize that, as an industry, we survive or fall together.
- We need to share our expertise with Congress and the FTC. No one knows kids better than members of the children's Internet industry. The more we share our knowledge and expertise, the better Congress can legislate in this area, and the better the FTC can administer those regulations and advise Congress.

An analysis of COPPA, how it works and why it was adopted is included in the appendix. I divide the issues addressed into two areas: data collection and interactivity.

Sites should have to jump through many hoops before they are permitted to collect and share personally identifiable information from children. They don't need to collect personally identifiable information, other than e-mail addresses. And sites should have a very good reason before being allowed to collect more. Parents agree wholeheartedly.

But it would be very helpful for Congress to enable a study on what information is being collected, how it is being used and what parents really want. Most of what exists is more anecdotal than scientific. Parents send me about 600 e-mails a day, in my role as author of the leading book for parents on children's Internet safety and privacy, The Parent's Guide to Protecting Your Children in Cyberspace (McGraw-Hill, 2000), and in my position as Executive Director of Cyberangels (the world's largest Internet safety, help and education group), and President of WiredKids.org (which includes UNESCO's online safety project for the U.S.). They care about finding reliable and safe sites for their children to enjoy online. They care about spam (unsolicited junk e-mail, often linking to adult content sites), more than any other single issue. They care very much about their own and their children's privacy. I am not sure that they care about providing offline consent, or online credit card or similar identifiers for their children to be able to chat or use interactive community tools at sites that have adopted safety guidelines and procedures.

With respect to interactivity, requiring the highest level of consent from parents before children can use chat, e-mail, instant messaging, and the like was designed to address the danger posed by pedophiles and other bad actors. But there are two things that can address it even more effectively.

One is educating our children on smart surfing practices. We, at WiredKids.org, working with Cyberangels, are designing a curriculum for teachers to use in the classroom to teach safe chatting and online communication skills. Congress can be very effective in helping promote online safety education, especially for children. Our Teenangels program educates teens to teach other teens and children about safe surfing. This can be expanded nationally, with support from schools and community groups. Our new online safety video for children and teens will teach practical safe surfing tips. But we need more programs like this and funding for these programs, in order to be effective.

Two is getting sites to use safe surfing practices, such as moderated chat, and parental approved e-mail and instant messaging correspondent lists. Closed list of permitted correspondents, like the Buddy list used by AOL and the Cyberfriends list used by Surfmonkey are good examples of how parents can pre-clear certain real life friends for communication, while locking out strangers. These kinds of interactivity, when designed with children's safety in mind, should be permitted without having to get parental consent. Not, in my opinion, that parent's won't give the consent if they took the time to focus and respond, but because parents aren't bothering to respond. This is an issue that providing the FTC with more discretion can resolve.

Perhaps, by providing the FTC with more discretion in this area, the sunset provision for "email plus" consent may be extended, and certain types of activities at safe sites can be permitted with a reduced level of consent or notification. Sites could submit their practices to either the FTC or a safe harbor entity for approval. This would allow sites the flexibility they need and provide incentives for adopting safe surfing and ethical privacy practices.

For example, the FTC should have been permitted to allow sites which have designed a safe chatting setting, such as clear site rules, trained chatroom moderators and use of technology to filter out certain prohibited terms, to avoid the onerous task of getting prior parental consent. Sites should have been permitted the option of presenting a package safety and privacy solution and approach to the FTC for approval, and for exceptions to the prior verifiable parental consent rule.

The way it currently operates, a site can get parental consent to any interactivity, no matter whether it is designed with the child's safety in mind. This actually provides a disincentive for safety and privacy practices at the site. And given the cost of moderating children's chatrooms, it is a choice many sites are making.

If the FTC had more discretion, it could approve these systems and permit the sites that use them to avoid the full-fledged verifiable consent mechanisms. It would encourage more innovation in this area, and keep our children safer at the same time. Sites which were approved could boost traffic by providing chat and interactive features children enjoy, which would in turn improve their financial position. This would provide further incentive for developing safe programs for children.

Offline consent mechanisms, digital signature development, school-related programs, and central registries are essential to helping the children's Internet industry navigate the current challenges it faces. But giving the FTC more discretion to provide exceptions to the verifiable consent requirement is one of the most important changes that could occur, and one of the most important things that this Subcommittee can recommend.

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.

APPENDIX
COPPA DEVELOPMENT AND ANALYSIS

The Children's Online Privacy Protection Act ("COPPA"), and the regulations thereunder which took effect on April 21, 2000, require all commercial sites to take special measures when they collect personal information from children or allow children to use interactive features, such as e-mail, instant messaging and chat (if they could share personal information with others using those tools). Many sites are confused about what the law provides, since it uses the word "collection" and they see that as something affirmative they are doing. But "collection" includes letting children use e-mail accounts or post messages publicly through a chat room or discussion board, as well as fill out forms. And it has nothing to do with adult content children may see online.

While the regulations are aimed principally at the children's Internet industry, they are fully effective against general interest sites with actual knowledge that a child is using their services. Few lawyers, even among experienced cyberspace practitioners, understand the children's Internet industry and the regulations and safety concerns that apply to it. But failing to understand what information can be collected from children, how it can be used, and what must be accurately disclosed to parents has cost many companies dearly.

There are two issues dealt with by COPPA and the existing consumer protection authority of the FTC. One is privacy, the other is safety. Both are regulated by the FTC, although states are permitted to enforce consistent local laws. In brief, privacy relates to the collection, maintenance, or use of personally identifiable information from children 12 years old and under. Safety is impacted, legally, when a child under the age of 13 is able to share personally identifiable information with others online.

The safety concern is that someone such as a pedophile may be able to contact the child either online or offline because the child has shared such contact information, whether intentionally or not. Last October, the FTC promulgated its final regulations implementing the Children's Online Privacy Protection Act of 1998 (COPPA). Yet few were aware that the FTC already had the ability to enforce the privacy and safety concerns noted above, and has expressly set forth the parameters of that authority since mid-1997.

The salient document is the " Kids-Com Letter." Online since February 1995, KidsCom was one of the first children-only sites on the Internet. It did not use "cookies"-which glean data about site visitors-to gather information, but collected data through registration forms, contests, and pen pal programs. It was directed at children from ages four to 15 and came under criticism for its collection practices. (As a result of the FTC investigation, KidsCom revamped its site and is very popular among parents and children.)

In May 1996, the Center for Media Education, a consumer watchdog group, filed a petition with the FTC requesting that the agency investigate KidsCom and bring an enforcement action against it. CME asserted that KidsCom's data collection practices violated Section5 of the FTC Act's "anti-deception" laws in two ways. First, KidsCom collected information from children without accurately disclosing the purpose, and second, KidsCom failed to disclose that it was paid to endorse certain products. In July 1997, the FTC issued its findings in a letter. The FTC determined that KidsCom's disclosure was "likely" inadequate and misleading, but declined to take any punitive action against KidsCom since the company had already changed its data collection practices and cooperated in the FTC investigation. The FTC discovered that KidsCom was sharing information collected from children with third parties, though this information was provided only in an aggregate form (e.g., 10-year-old boys from New York preferred baseball over football).

In issuing this ruling, the FTC for the first time publicly announced its guidelines for data collection from children on the Internet. Relying on '5 of the FTC Act, which prohibits unfair and deceptive practices in or affecting commerce, the FTC stated: "It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose (e.g., to earn points to redeem a premium), when the information will also be used for another purpose which parents would find material, in the absence of a clear and prominent disclosure to that effect."

Second, the FTC stated, when collecting personally identifiable information, "adequate notice" of such practices must be given to a parent because of a child's limited ability to understand the disclosure. "Adequate notice" requires disclosure of: (1) who is collecting the personally identifiable information; (2) what information is being used and

for what purpose it is being used; (3) whether it will be disclosed to third parties, and if so, to whom and in what form; and (4) how parents can prevent the "retention, use or disclosure" of that information.

Third, the FTC articulated its "unfairness" test for Internet child safety, noting that the disclosure of children's personal information to third parties is of particular concern, and that parents must be given adequate notice of such use and the opportunity to deny their consent to it. The FTC has had broad regulatory powers when dealing with safety issues, under its unfairness authority in section 5. Under that section, a practice is unfair if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and not outweighed by countervailing benefits to consumers or competition.

In its fourth and final principle, the FTC criticized KidsCom's endorsement practices as misleading and deceptive. KidsCom had "New Product" areas, where products were reviewed and endorsed. What it had not disclosed was the fact that, in exchange for an endorsement, product manufacturers had to contribute at least $ 1,000 worth of product, which was used for premiums and prize redemptions. The passing off of an advertisement as an independent review or endorsement is a deceptive practice under '5 of the FTC Act. KidsCom failed to clearly and conspicuously disclose that the product information was solicited from manufacturers and printed in exchange for in-kind payment.

Following the issuance of the KidsCom Letter, the FTC broadened its principles to include offline consent for children 12 and younger anytime their personal information may be shared online in chat rooms or similar third-party communications, and before any site collects and stores their personal information, even an e-mail address.

The adoption of COPPA was in direct response to the lack of industry compliance with the law as articulated by the FTC in the KidsCom Letter.

In June 1998, the FTC presented its Privacy Online Report to Congress, documenting the online collection of personal information from children. The FTC rearticulated its prior concerns that collection of personal information from a child under the age of 13 without informed parental consent would be a deceptive trade practice. The FTC reported to Congress that even in chat rooms, children innocently and without request may reveal where they live or go to school or their real e-mail addresses. The FTC informed Congress that parents need to understand the risks and consent to any such collection and disclosure of personal information. Congress apparently agreed, and wasted no time in acting on the FTC's report. Within months, COPPA was law.

COPPA requires that commercial Web sites obtain verifiable parental consent before collecting personal information from a child under the age of 13. Failure to obtain such consent is an unfair and deceptive trade practice and can result in fines of up to $11,000 per occurrence.

COPPA applies to commercial Web sites, online services "targeted at children," and any online service operators with actual knowledge that they collect personal information from a child. (Actual knowledge can be as simple as a child's sharing her grade or age in a monitored general audience chat room on a site, or can be supplied by an e-mail or phone call from concerned parents who object to the collection practices on behalf of their child.) Personal information includes such items as full name, home address, e-mail address, telephone number, Social Security number, or any other information that the FTC determines "permits the physical or online contacting of a specific individual."

The regulations require covered operators to:

1. Provide notice on the Web site of what information is collected from children, how information is used, and the Web site operator's disclosure practices for such information (notice this applies to all information, not just "personal information");

2. Obtain verifiable parental consent (which requires more than a mere e- mail consent from the parent) to collect, use, or disclose children's personal information before it is collected from the child, with certain exceptions and special rules for newsletters and internally used information;

3. Upon request, provide parents with a description of the types of information collected from their child, or the actual information obtained from their child, and the opportunity to refuse to permit the further use, maintenance, or

future collection of the child's personal information. Thus, in addition to having to obtain initial consent from the parents, if a parent withdraws consent at any time, the operator must remove that child's personal information from the system;

4. Cease conditioning the child's participation in games, contests, or any other activity upon the disclosure of more information than is reasonably necessary to participate, including permitting parents to allow the site to collect personal information but refusing to let the site share the information with third parties;

5. Maintain reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from children."

The law also details three different levels of consent, as well as the various types of notices required under the statute, which cover everything from the content of those rules to the look and placement of the link to the privacy policy displayed at the site, as well as the technical requirements for obtaining "verifiable" parental consent.

All websites need to look hard and thoroughly at their collection practices. Even if COPPA doesn't apply to the site, they may still run afoul of the FTC Act if their privacy policy does not accurately and completely disclose what personal information they collect from their users and what they do with that information. If they collect personal information that includes a person's age or grade or similar information, they may then have actual knowledge that they are collecting personal information from a "child" and need to comply with the full panoply of COPPA regulations. Even if they don't overtly request that information, if they have monitored chat rooms or discussion boards at which a user may disclose information from which the site should know they are under 13, that may provide the requisite knowledge under COPPA.

If the site collects any personally identifiable information from its users or provides any means of public disclosure of such information (such as through an e-mail service, chat room, discussion boards or instant messenger service), and the site is alerted that a particular user is a statutory "child," then the site must also comply with COPPA.

Banner advertisers and network advertising companies are covered by COPPA and its regulation if they advertise at children's sites and collect personal information from children who click through from such sites. They are also covered if they have ownership or control over such information collected directly at the children's sites. Advertisers at general audience sites may also be covered by COPPA if they collect personal information from people who click through, and that information discloses that the visitor is a child.

We have learned that many companies are collecting data from their Web site visitors without knowing why they are collecting it or if they are using it properly. Unless companies are under investigation or have heard of another company under investigation, their legal departments rarely communicate with Webmasters. With this new law on the books, all commercial Web sites must be vigilant in ensuring that the rights of parents to notice and consent are honored. If such companies ignore parents' concerns regarding privacy and advertising, they will have to face more than the FTC they will be facing the even tougher scrutiny of a disgruntled parent.