December 29, 2011

Donald S. Clark, Secretary
Federal Trade Commission
Office of the Secretary, Room H-113 (Annex E)
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Re: COPPA Rule Review, 16 CFR Part 312, Project No. P104503

Dear Secretary Clark:

WiredTrust (WiredTrust.com), WiredSafety (WiredSafety.org) and Parry Aftab, Esq (in her individual capacity as a child advocate and privacy and security lawyer to the children's digital industry) are filing this comment on behalf of themselves with contributions from certain children's Internet industry clients of WiredTrust and Ms. Aftab. We appreciate the willingness of the FTC to solicit comments from the public, advocacy groups and policy and industry leaders to the Proposed Amended Rules for COPPA. We also recognize the hard work of FTC staff and executives and their continued commitment to engage all stakeholders and remain accessible over the years.

While we are not strangers to the FTC and Congressional Representatives, it may be helpful to put our comments into perspective. We approached these comments from the privacy and security law perspective, as well as child and family advocacy and safety perspective. In addition, WiredSafety[1] receives emails from parents and young people alike requesting help on COPPA, privacy and problems encountered online and through the use of digital technologies, so we also address the public's concerns and confusion. And WiredTrust[2], a private best practices and risk management consulting firm, offers practical insight and input from its many clients in the children's digital industry.

Parry Aftab[3], WiredTrust's and WiredSafety's founder and chief executive, together with her former law partner, Nancy L. Savitt[4], was actively involved in the drafting of COPPA and the policy issues emerging from the Kidscom.com matter filed in 1997.

We support many of the FTC proposed changes and the decision to leave certain provisions unchanged. These address the legal and practical concerns of many professionals in the field. In particular, we highly support the decisions (for the reasons put forth by the FTC) not to increase the age of a "child" to teenagers and not to change the "actual knowledge" standard.

However, we have concerns about certain of the proposed changes. Those are discussed, in detail, below, but include:

- Retaining Email Plus - We believe that "email plus" is still needed.[5] While we can see it being phased out as better and less expensive alternate methods are developed, killing it to encourage the development of alternatives leaves children, their families and the industry without a stop-gap solution. It cuts them off until someone develops an effective method of obtaining requisite parental consent for less-risky uses of personally identifiable information. No one benefits from that. In addition, email plus is the preferred

method to obtain parental consent for online contests and promotions where the prize must be mailed to the child, offline. The Promotional Marketing Association, Inc.'s (the "PMA") comment filed in response to the Proposed Rule discusses this issue in detail. We concur with this additional reason to retain email plus.[6] Our full-analysis of the need to retain email plus, at least in the short term, is set forth below.

- If Email Plus is Abandoned, a Sunset Provision Should be Adopted - However, if "email plus" is abandoned, a sunset period of at least eighteen months should be established to allow other solutions to be designed, developed, tested and approved. Promises of technology solutions almost ready for launch are too often the digital equivalent of "the check is in the mail." Many promising technologies are just that – promises. They are less often delivered than we hope.

- Data Collected in Compliance with the Current Rule Using Email Plus Should be Grandfathered – If email plus is abandoned in its entirety, unless we expect the children's digital industry to start from scratch with current users for whom email plus notifications have been given and consent obtained, existing data should be permitted to be used for the purposes for which is was collected (assuming it was collected in compliance with then applicable law). The risks are lower when dealing with this issue, as well, especially because as the children age, in all likelihood, they will graduate to "teen pastures."

- Expansion of Categories of "Personal Information" are Not Necessary and are Problematic – The proposed expansion of categories of information, standing alone, that constitutes personally identifiable information is problematic. Classifying screen names and user names, zip + 4, all IP addresses, voice, and other identifiers that cannot lead to the clear identification of a preteen in real life or allow the unauthorized contacting of a preteen ignore how technology currently works, and does not realistically address risks. Instead of expanding the list of types of data that falls within personally identifiable, we believe it is time to move to a "use" regulatory approach. (A more complete discussion of the "Elephant in the Room" of "use" regulation is included below.)

- The One-Time Use Exception for Notifying Parents When Preteens Win a Contest Should Not Be Changed – The Promotional Marketing Association, Inc.'s comments raised the concern that subtle changes in the language of the Rule had the potential of changing the Rule permitting the one-time use exception for online contact information ("OCI") collected from a child.[7] Under the new proposed language, assuming it was an intentional change as opposed to a typographical error, the Rule is proposed to now cover OCI of a child, and would no longer be available to cover situations where children supply their parents' OCI to be used to obtain express consent for delivery of a prize or other promotional product for the child.

- Requiring all Operators to Provide Contact Information Creates More Confusion, Not Less – The FTC proposes to require all operators to provide their own contact information, not relying on one entity that shall act for all site operators. As discussed in more detail below, we believe that this will result in duplicative communications and increased confusion. The one point of contact has worked well in practice and we believe need not be changed. Requiring that all operators comply with COPPA and provide the requisite COPPA notices and obtain requisite consent may be a more effective way to address any concerns and strengthen compliance. Any "just in time" notices and policies would then contain the requisite contact information that that operator.

Putting It in Practical Perspective:

As we look at the costs, benefits and needs for COPPA Rule changes, we would be remiss if we failed to examine the practical costs and challenges these proposed changes may bring to an already struggling industry. Most

industry members share the FTC's commitment to protecting children in the online environment. In certain instances, we believe the proposed changes, or the manner in which the changes are structured, will have unforeseen ramifications, and unintended and undesirable effects on the children's digital industry and other online platforms and forums. It is important that the proposed changes are considered in this light.

While burdens on the industry will never outweigh risks to our children, many concerns being addressed by the proposed changes may be mere speculation and often are not supported by examples of ineffectiveness or harm. We shouldn't have to resort to speculation. In the 11 years since COPPA has been in effect, we have learned what risks are real and which are not. It is important that we look to what we know when recommending change.

The "Health" of the Children's Internet Industry:

Historically, in the days of the early Internet, the children's industry fell into three distinct groups: the big household name companies (the Disneys, Sesame Streets and Viacoms of the world) looking to build an online brand to complement or perpetuate their offline brands; the middle tier of Internet start-ups that had gained substantial popularity online (Headbone and Freezone, etc.); and the smaller operators (moms and pops, emerging start-ups and innovative networks without funding).

There was no successful business model for the children's industry online. Everyone was looking for that "magic bullet" to get parents to pay for online content directly, instead of having to scrounge for advertisements and sponsorships or raising capital until a better idea came along. But that better idea was unreachable until Club Penguin managed to drive the subscription model effectively, almost a decade later.

The Internet market crashed in March 2000, barely a month before the effective date of COPPA, April 21, 2000. The children's sites were substantially more affected than general audience sites, with the mid-level children's websites affected most of all. Most were wiped out completely.[8] The bigger companies could weather the storm with other sources of funding and diversified operations and rely on their branding. The smaller companies operated on a shoe-string from their garages, without employees or access to the financial markets at that point in their development.

To compound the problem, the VCs backed away from children's and tween sites in particular. Funding sources and promises dried up. And advertisers were unwilling to support children's sites because of the low rate of return of Internet advertising at that time, particularly targeted at pre-teens.

Although they had eighteen months to prepare for COPPA's requirements (from its enactment date of October 1998 to its effective date in April 2000), given the state of the Internet market, few middle-tier sites and networks survived. And the middle-tier is often where the best innovations occur, new models and offerings developed and opportunities are identified. Without them, children are deprived of many rich opportunities and activities online for education, entertainment and safe interaction.

COPPA verified parental consent was costly (costing upwards of $40 per user, to obtain) and difficult to obtain at any price.[9] Parents were reluctant to provide credit card information, and the toll-free consent model (which we developed for Headbone in early 2000) proved expensive and clunky, while offline fax and snail mail options frustrated the users who wanted faster approved access. While the FTC and the industry struggled to find a way to make COPPA work for all levels of preteen sites, "email plus" was adopted.

The industry is facing hard times once more, along with most of the nation and world. In addition to the economic challenges, the industry is still struggling to find workable business models. As families face economic challenges as well, there is less disposable income for online activities and fewer families have access to credit cards. In addition, the more technical these solutions and models become, the more likely lower-income and techno-challenged families are left out in the cyber-cold. It remains a struggle, one in which WiredTrust, WiredSafety, and

Parry Aftab, herself, are deeply engaged. We don't have the answer yet. No one does. But we need to make sure that we are not throwing the potential of robust and valuable digital uses out with the COPPA-compliance bathwater.

With this in mind, while some other proposed changes appear to work on the surface or in isolation, those of us who have practiced in the COPPA/children's privacy, safety and security space since the mid-90's have learned that the devil is in the details. Unexpected consequences to well-intentioned and carefully thought-out strategies are very common. Putting things into practice is more challenging than many expect. The ability of preteens to "game" the system grows by the minute. Confusion abounds. And, things that appear fine on the surface may wreak havoc in practice when dovetailed with other seemingly innocent provisions.

We have to proceed practically and understand all implications of proposed changes. We have to make it clear. We have to understand the challenges faced by the providers who want to comply, provide a safe, private and responsible network or application. We have to make it work.

Several proposed amendments are likely to create confusion among consumers and the providers. These should be clarified when the COPPA Rule is finalized to minimize the likelihood of confusion. These include:

The addition of the permitted collection and use of parental contact information provided by preteens, even when not required under COPPA. Without question, this addition (although welcomed since it now brings many sites' practices into compliance) will cause parents and operators to think that COPPA notices are required, when they are not. It should be clarified as being voluntary, only.

The new requirement that all operators provide contact information on the site will not assist in dispelling confusion. It will create havoc. As it stands, a distraught parent will reach out to anyone and everyone they can find to help. WiredSafety and Parry receive thousands of emails a day, many from parents who have copied the FBI, other advocates or law enforcement agencies, people in the media, elected officials, non-profits and even the FTC on their issue. While we understand why they do it, hoping that someone will address their concern, WiredSafety and Parry Aftab, personally, have adopted a policy of ignoring such mass-copied communications. Their resources and time are limited, and if others are being copied it is expected that someone else can address it effectively.

This same problem will exist here. Everyone in the chain of operators and providers will be copied on lost password requests, access issues and questions about how the game works or when a new product will be released. No one knows where to direct their communication. So all will be contacted. Like WiredSafety and Parry, these operators have priorities and need a strategic method of addressing legitimate concerns that fall within their competency. Otherwise, they won't be able to do their jobs.

The one contact point worked.[10] The people manning that contact are trained to address and air-traffic-control the inquiries. There is no reason to think that it will not continue to work. Anything else, while well-intentioned, only makes matters worse. It won't help parents, or consumers. It will only confuse them.

When the operator is permitted to share preteen's personally identifiable information (as well as parental contact information) with law enforcement and child protection agencies, by making it clear that the safety and security exceptions of COPPA override the new limitations on use and disclosure.

Preventing operators from sharing the users' activities on their sites, properties and when using their applications with the affiliates operating their different platforms (website, virtual world and mobile app, for example)

Email Plus:

We believe email plus should be retained as it is time-tested, and has proven to be effective and efficient. Alternative proposed methods of obtaining parental consent do not necessarily increase reliability but create barriers to the provision of consent by parents, create delays, and increase costs to operators. The result could well be to decrease children's participation on children's properties and also reduce the number of interesting children's sites made available by operators. We suggest that neither of these is a desired result and may encourage children to seek out participation on non-children's social sites. This result would be especially unfortunate since there is no identified "harm" of retaining the email plus Rule.[11]

While we commend the FTC on taking a bold step forward to encourage innovation, we believe that eliminating email plus at this time is premature and would not encourage innovation. Instead it will likely result in a reduction of innovative and valuable features available to children online. If US companies cannot bear the cost of immediately implementing a new method of obtaining parental consent or a previously approved, but expensive method, sites will shut down and children will be forced to visit sites from other countries that are not in compliance with COPPA or encourage children to lie about their age to use general audience sites and networks.

Admittedly, email plus is not a perfect solution, but it has been extremely successful at balancing the risks (which are limited because email plus is only used in cases where data is used internally and not shared with third parties) against the practicality of obtaining reliable parental consent from millions of parents. The FTC recognizes, by citing to our previous comment, the successful history and implementation of email plus by saying, "E-mail plus has enjoyed wide appeal among operators, who credit its simplicity. [citing to one of our earlier comments] Numerous commenters, including associations who represent operators, support the continued retention of this method as a low-cost means to obtain parents' consent."

We posit that nothing has changed in recent years to make email plus less effective than it has been. A replacement method should be promoted only once it is readily and commercially available. Today, there are no solutions that match the ease and effectiveness of email plus. In addition, any new technology will require time to be designed, developed, tested, and approved by the FTC, before it can finally be implemented by operators.

If a decision is made that email plus should be abandoned, we recommend at least a one and a half year phase-out period. This would allow ample time to spur thoughtful innovation and provide time for new methods to be designed, tested, approved, and implemented. The FTC previously recognized this length of time when COPPA was first enacted by providing operators until April 2000 to comply with its requirements.

In addition, if email plus is abandoned , what happens to all the data already collected and being used by operators in compliance with existing COPPA? Will it be grandfathered? If so, how and under what authority? The fact that the Rule does not provide for grandfathering, transition, or phase-in periods is highly problematic. New properties take years of work to build, even before launch. Existing children's online properties are complex in their programming and technological infrastructure. One change affects many things. The complexity of these properties and the sheer size of some of their online populations would necessitate grandfathering provisions since the business models underpinning those sites were built on the existing Rule. Even for less critical changes, lengthy transition periods would still be required in order to achieve compliance for technical and programming modifications.

We are not aware of any harm arising from the use of the email plus method. In fact, we believe this method of interacting with parents has been time tested and shown to be effective and efficient. We believe alternative methods of obtaining parental consent are neither desired by operators nor parents as replacements for this method. We believe the currently proposed alternative methods would not necessarily be more reliable than email plus, although they would have negative impacts; namely, they would set a high barriers for parents to provide consent, create delay, and be costly.

The fact the proposed Rule changes to permit a parent's email address to be used to provide notice per section 312.4 seems to indicate the FTC considers emailing parents at addresses provided by their children, to be effective and reliable. This implicit endorsement seems to run contrary to the proposal to eliminate email plus.

We would respectfully suggest that the FTC's expressed desire to spur technical innovation to replace email plus, surpasses the FTC's mandate. We believe the FTC's mandate is consumer protection and that Rule changes should be to address consumer harm. We would suggest there is no harm here.

To discuss the elimination of the method further:

- Some proposed replacement methods are no more, or not significantly more, reliable than email plus - - faxed signed documents and electronic scans of signed forms, for example. Toll-free numbers and video-conferencing do not ensure the person on the other end of the call is the child's parent or legal guardian.
- Email plus does help ensure the operator has received a functioning email address. This is helpful in the event the operator wishes to contact a parent regarding a security issue.
- We believe the alternative methods for obtaining parental consent presume parents own or have easy access to certain required equipment (i.e., scanners, faxes, video conferencing equipment). This may well not be the case. These methods are also intrusive and time consuming for parents and are likely to create a barrier to their provision of consent. These barriers could have a chilling effect on children's online properties.
- The proposed methods would create delay in child participation in some aspects of online games, especially successful ones that have large communities of child users. For example, consider what would happen in these communities, especially on high activity periods –e.g., Thanksgiving, December 25th, etc. when manually intensive consent methods are required to enable online play.
- From the operator's perspective, the proposed alternatives may necessitate reformulation of business models due to the heavily manual, time consuming and expensive nature of obtaining parental consent.

In addition, there are enormous staff resources and additional costs required when these changes are made. These greatly increase operators' staffing, training, and related compliance requirements and costs. Although these changes may not be as time demanding as addressing technical and programming issues, operators would need time and resources to respond.

The Elephant in the Room – "Use":

The FTC has held several hearings on COPPA. We have been fortunate to have been asked to contribute to and participate as experts at those hearings in most cases. The dedicated FTC staff has devoted years to understanding the emerging technologies and their capabilities, as well as network practices. Yet, as soon as any of us grasps one technology, it is out-of-date and replaced with another, or 100 more. As we try and become granular with the different digital tools and applications and how they could be abused or used in unintended ways, perhaps it is time that we step away from the *specific technologies* and their capabilities and look to the *use* of those technologies instead.[12]

COPPA in the early days was setting out rules. These rules told operators say what to post and where to post it. It instructed them on the size of the font and content to be included in the privacy policies. It explained what they could ask for and what they couldn't. COPPA was written this way because "soft" guidance of the Internet industry in the days preceding COPPA's adoption didn't work. The industry largely ignored the please, warnings and threats of the FTC to get them to voluntarily comply. In 1998 most Internet providers needed that level of guidance. But this, at least, has improved over the last thirteen years. COPPA has become ingrained in the development of most preteen technologies. Even if the operators don't fully understand the law, they know it exists and try to adhere to their understanding of COPPA. It's time that we treat the kids' digital industry operators as adults. Instead of trying

to micromanage the technologies, it's time we micromanage the *use* of data collected from preteens online, instead.

This approach, which has been adopted by the FTC in its explanation of the Proposed Rule in permitted use of information collected for the operation of the site, resolves several challenges:

- The technology changes by the nano-second;
- No two experts can agree on the capability of the technology to locate preteens in real life or be able to identify them in real life;
- The marketers and advertisers are always developing new ways to reach their markets and by targeting use, instead of the actual technology being used, the FTC can precisely control their activities;
- Devices, that may be overseen by governmental agencies other than the FTC, can be regulated if the use of data collected by the device is regulated, instead of attempting to regulate that device itself;
- Adopting a "use" viewpoint keeps COPPA evergreen, without the fear that it doesn't cover new technologies or capabilities of those technologies;
- "Use" can be measured now. With the assistance of tracking technologies of our own, how an operator uses data can be audited. The new audit provisions proposed can cover the requisite testing and certification of the site's practices. (This is something WiredTrust is already doing with its upcoming Socially Safe Audits and audited Socially Safe Seals.);
- By looking at "use" instead of the technology tool itself, the FTC can spur innovation in technology development and uses of all digital technologies;
- By focusing on the ways certain technologies can be abused, and denying their use to all COPPA-compliant providers, the FTC is using a bazooka to kill flies and at the same time, blaming the innocent and compliant members of the COPPA-regulated industry for the abuses of a few;
- By allowing compliant uses of existing and developing technology that would be prohibited under the Proposed Rule, these technologies will be enhanced to work in safer and more private ways;
- More ways to test "use" compliance will be developed and allow the FTC, advocates and parents to determine the trustworthy providers from the rest; and
- After 13 years and the third bite at the COPPA apple, we have all learned how to do this better, to protect our preteens more effectively and get parents on board – it's time!

In addition to focusing on the real issues – inappropriate marketing schemes, unfair behavioral targeting of our children and their safety, this allows all stakeholders to develop a more compliant and innovative industry.

The only challenge that remains to this approach is making sure that if personally identifiable information, however defined, is being collected, that it remains undisclosed and secure and deleted when no longer needed. That is a security issue and perhaps where we should be focusing our renewed energies. How secure is the data collected? And how can we improve on security at all levels. Just as important is the issue of how do we notify parents if there is a data-breach or if we believe that their child's personal data is at risk (perhaps from other users targeting that preteen for cyberbullying or harassment)?

We respectfully assert that more effort needs to be placed by the FTC on security and safety concerns, not just marketing practices. COPPA began with a dual prong goal – to protect children from the perceived risks form online sexual predators who might find their real life location from what they share or posted online and the Kidscom.com issues of unfair marketing to, and potential collection of personally identifiable data from, children. When we all helped in its drafting, we would consistently look to the issue of whether a marketer or predator could locate the child offline and contact them for their purposes.

Now, when all digital communications and interactions are tied to devices that gather and store data unknown to most users, from a Word document's metadata, to a digital camera's geo-location, time and device owner's

information[13], to facial recognition capabilities of images and videos, to static IP addresses and handheld and mobile devices that can identify the approximate (or potentially, exact, location of the device or user, or from where the communication was submitted), we have to look beyond the technology. We have to look at tools, practices and uses to make things safer.

Clarifying Definitions:

The FTC proposes to modify the definitions of a number of key terms. In general, we are pleased by the FTC's efforts to streamline lengthier sections to make them more understandable and accessible. We offer our thoughts on some of the specific changes in this section.

a) Personal Information

The FTC proposes to modify and expand the list of things that are deemed to be personal information.

One suggestion presented by a commenter, and addressed by the proposed rules, would make "any collection of more than twenty-five distinct categories of information about a user" automatically deemed to be personal information. The FTC was right to dismiss this quantity-based approach. With this in mind, instead of listing technologies and categories of information that have the potential to be personally identifying, we look at the their use and implore the FTC to do likewise. We recognize this will be harder for the FTC, safe harbors, advocacy groups, and corporations themselves. We also acknowledge the risk involved in allowing more people to collect more information as it may allow inadvertent disclosure and accidental breaches. However, these issues can both be addressed through heightened security directives, clear dovetailing with data breach and disclosure rules, and heightened auditing practices on the part of the FTC, compliance agencies, advocates, and groups such as ours.

1) The revised list introduces "screen names" or "user names" as personal information where they are used for a purpose other than to maintain the technical functioning of the website. These terms are not always used interchangeably by the industry, which will cause confusion. User names and screen names are not usually or necessarily the same thing, nor do they serve the same purpose. In children's online properties such as a virtual world or game:

- User names are typically required to be unique to every user in order to protect the integrity of game and the accounts of the players. User names are therefore precise, accurate and consistent since they are required for entry onto the site.

- Screen names are not necessarily unique nor are they required to be displayed in the game in a consistent fashion.

- Children's online properties are typically structured to not collect personal information (as it is currently defined), with the result that no personal information is associated with either the screen name or user name on site.

Our work advising and working with the industry has taught us that practically screen names do not necessarily have a one-to-one relationship with a user. For example, the game may base screen names on the name a child selects for their online character or avatar. This means children having many avatars will have many screen names, and their screen name will change in the game as they change avatars during a playing session. Avatar names are also not always required to be unique, which means many screen names will be duplicated without limitation throughout the game. The result is that these screen names are not user specific and are incapable of identifying a specific user. For these reasons we believe that this section requires further clarification of what is meant by a screen or user name with a focus on whether they are personal and have the potential to be used to contact an individual.

From a policy perspective, we believe the FTC is concerned with the "name" that is displayed online (which we will call a "screen name") since it would be viewable by other players. (We note that this criteria of being "viewable" is not referenced in the definition, but we think it should be if this is the intent.) Screen names may be displayed in numerous different ways within an online game depending on the intended purpose or functionality of the section in the game (i.e., where players need to identify each other in order to play). In sections of the game where more specificity is desired to allow players to identify each other, the game may add to the displayed avatar name, other details such as portions of the user name, for example. Moreover, the extent to which such added details (portions of a user name, in this example) are displayed may depend on the relationship between the users who are viewing the screen name. For example, if users are not designated as "friends" within the game, the displayed screen name may only add truncated portions of the user name to the avatar name. If users are designated as "friends", a more fulsome version of the username and avatar name may be displayed.

Surely, all of these screen names should not be considered "personal information", especially if none of them is tied to any personally identifiable information on the online property in which the screen name is created and displayed. The current Rule and definitions make a screen name personal information if it includes an email address, or if it is otherwise combined with personal information (e.g., first and last name). We think the current Rule is clear and protective of children and should not be changed.

In one paragraph of its discussions, the FTC states, "…Accordingly, an operator may allow children to establish screen names for use within a site or service. Such screen names may be used for access to the site or service, *to identify users to each other* [emphasis added], and to recall user settings. However, where the screen or user name is used for purposes other than to maintain the technical functioning of the Web site or online service, the screen name becomes "personal information" under the proposed Rule." This would seem to indicate that in-game viewable names that permit users to identify each other would be exempt from the definition (i.e. they would not be personal information). If this is the case, then much of the discussions above become moot since screen names, displayed in their various forms and in various areas of an online game, are typically included only for the purpose of allowing users to identify each other for in-game purposes (for example, for chatting, to post high scores, to allow players to carryout cooperative games).

However, if this is not the FTC's intent, then taken to its logical conclusion, all screen names would be captured by the new definition of personal information and the only way to not trigger the definition would be to have the game randomly allocate a new screen name to a user every time the user logged into the game. Not only would a child user not know their own screen name from one session of game play to the next, no other players in the game would be able to identify any other player. This would completely end the social and cooperative play aspects of children's online games. We feel this would be an undesirable and disastrous result. We do not think is the intent of the FTC, which itself has noted that children seek social environments and has encouraged operators to develop age-appropriate social communities.

2) The revised list introduces a paragraph on "persistent identifiers," paragraph (g), which we believe requires clarification. The proposed definition exempts screen names from becoming "personal information" if they are used for functions other than or in addition to "support for the internal operations of the Web site or online service", which term is then further defined. We are unsure of the scope of this exemption.

If the reason the FTC added this new category of personal information was to address behavioral profiling and advertising, we think this should be done directly and explicitly. A stand-alone prohibition could be used, as suggested above. Alternatively, the definition of personal information could be structured to capture only those user name names or screen names which the operator: (i) collects or uses for behavioral advertising or profiling purposes; or (ii) discloses to third parties for behavioral advertising or profiling purposes.

In addition, the exemption may not include other valuable uses such as collecting information about children in order to protect them from themselves or each other. While we respect the stated purpose of this paragraph, which is to prevent behavioral ads, we believe that there may be unintended consequences as it is written. We believe that the approach should pursue the distinction between the uses of the persistent identifiers. This section is an example of where the FTC focuses on use of information to combat the problems that strictly limiting collection of information introduces when that information is used innocently.

Furthermore, many persistent identifiers, such as cookies, are used to comply with COPPA (such as a cookie to block an underage user from bypassing an age gate) and that functionality might be limited by the revised language. Persistent identifiers are also used to increase site safety, for example by permanently banning a known hacker or child predator from a site. Without some way of tracking and identifying these users the end result will be a decrease in site safety for only a theoretical benefit to children. Limiting the uses for persistent identifiers is therefore a more fitting approach.

This approach will also better serve the addition of geolocation data which has been added as paragraph (j). Collecting geolocation data can be invaluable in a case where a user threatens self harm, is missing, or threatens another user or the site. Prohibiting its collection would impede these and other valuable services. With regard to geolocation data, we believe a distinction should be drawn between instantaneous locations and databases of locations that can be used to reconstruct a user's path.

3) The revised list introduces a paragraph, paragraph (i), that includes photos, videos, and audio files as personal information if the file contains a child's image or voice. The revised language needs to be clarified regarding what exactly is meant by "a child's image." For example, we do not believe that an image of a child which has had the face blurred using tools provided for that purpose or one that has been converted into a cartoon, sketch or other graphic (as many tools now facilitate[14]) should qualify as a child's image as it does not identify the child and cannot be easily subjected to facial recognition analysis. This would allow preteens to "personalize" their online space without putting themselves at risk for privacy or marketing violations or safety.

Voice files are a more practical problem. We believe that they should not be categorized as "PII" for the purposes of COPPA. Many preteens are creating animations, presentations, vocal performances and other multi-media projects online to share with others. While the risk of using a preteen's clear image in still photos or in video formats is obvious, the risk posed by allowing a preteen's voice to be heard is not. Instead, it would curtail very creative and valuable uses of the digital networks by preteens. In the sixteen years since Parry Aftab and the WiredSafety volunteers first began helping victims of online abuse and cybercrime, neither has once encountered a risk related to the online audio files of a preteen.[15]

If the FTC's concern is that a preteen may give away their personally identifiable information in an audio communication, by addressing that directly, providers and operators can screen vocal content for COPPA-identified risks. We do not believe that the FTC intended to prevent the use of voice-overs to presentations online, or the narration of stories or multi-media projects. To our knowledge, no one in the children's digital industry is matching voice or audio files to attempt to identify or communicate with a specific child or determine their identity. To the contrary, many are exploring the use of vocal recognition technologies to prescreen the age of a user and either screen for minors, or screen out minors.

A similar issue that may arise in the future is how to treat other types of files (such as Word files) that may have embedded information in them. One solution is to require operators to strip out meta data from files uploaded by users. This will also prevent location data appended to photos from accidentally being disclosed. This type of solution, as well as limiting how files can be used by an operator (for example, restricting facial recognition analysis) will provide a more future-technology-proof rule.

4) The proposed revised Rule introduces a paragraph, paragraph (h), which makes an identifier that links the activities of a child across different sites personal information. This will impede functionality that has come to be expected by many users. For example, sites directly affiliated with each other or owned by the same company may want to share login information or points among their properties or across platforms. We no longer live in a site-by-site world and big companies have multiple sites and brands.

There is concern that the proposed Rule seems to ignore that some children's online properties are related to one another and are operated by the same or related entities. In cases of affiliated properties, the operator may reasonably and legitimately wish to provide functionality between those properties and, assuming the required principles of disclosure have been met, such inter-functionalities should be permitted without verifiable parental consent. Some examples of such inter-functionalities include, transferring virtual prizes or currency to a virtual world from a related game application, transferring virtual items to a virtual world from a related e-store site.

For this to be effective, however, we support a requirement that sites should have to disclose their relationships with each other and with the various platforms that they use.

We reiterate that we support the policy that parental consent is required for persistent identifiers, identifiers linking activities across online properties, and geolocation data used to target behavioral advertising or create profiles for advertising purposes, and for the sharing this data with third parties for these purposes. We note that the FTC has articulated that the new definitions found at (g) (persistent identifiers) and (h) (identifiers linking a child's activities across different sites or online services identifies) are targeted to address these behavioral advertising and profiling uses.

We believe that there are legitimate functions that should be permitted and should be excluded from the definition: for example, amassing persistent identifiers for evaluation or statistical analysis of a property either by the operator itself or through the operator's authorized service provider would be an appropriate activity. Another example would be to permit inter-property functionality across an operator's related online properties and platforms. Similarly, using geolocation data for evaluating a property's popularity in a given geographical region, or for improving service would be appropriate uses of the data.

Accordingly, we recommend that the proposed paragraphs (g), (h) and (j) should be revised to specifically address the problematic uses, and the following are sample revisions.

(g) a persistent identifier, including but not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier, where such persistent identifier is collected, used or disclosed to third parties for *user profiling for advertising purposes or behavioral advertising targeted to children [emphasis added]*;

(h) an identifier that links the activities of a child across different Web sites or online services for *user profiling for advertising purposes or behavioral advertising targeted to children" [emphasis added]*;

(j) Geolocation information sufficient to identify street name and name of a city or town *where such information is used for user profiling for advertising purposes or behavioral advertising targeted to children [emphasis added].*

Finally, the revised list of Personal Information omits the catchall provision that was previously in this section as paragraph (f). Although it may be sufficiently addressed elsewhere in the Rule, we question whether this was an inadvertent omission or typographical error. If not, perhaps an explanation of why this change was made would be helpful to practitioners and operators alike.

(c) Site directed toward children

The FTC proposes a number of minor changes to the definition of a "Web site or online service directed to children" and we agree with the addition of the phrase "child-oriented activities," however, we oppose the inclusion of "music" and "animated characters" without more clarity. We also oppose the phrase "presence of child celebrities or celebrities who appeal to children" on two grounds:

- First, we disagree that the mere presence of a child celebrity is indicative that a site is directed toward children, even as only one of many enumerated indicators. Many fan sites are set up on existing preteen sites by representatives of young celebrities. If a fifteen-year-old pop star has an account on a general audience teen site, does that indicate that the site is for preteens and COPPA applies? If the change is accepted, sites will be reluctant to permit popular young celebrities to create a fan page on their site for fear that their presence will make it more likely they are deemed "directed toward children."
- Second, as the title of the section states, we are looking to define what makes a site "directed toward children." The additional of this new proposed enumerator including the use of celebrities who "appeal" to children sets a new standard. Does Lady Gaga appeal to children? Does Katy Perry? What about Taylor Swift? Beyonce? Rihanna? Maroon Five or One Republic? Justin Bieber? Adele? Lady Antebellum?

The same argument holds true with "music" and "animated characters." All we need to do is listen to the bands and singers our preteens enjoy to understand that they like what their older siblings and counterparts like. What about movies? Is Twilight a problem? War Horse? What about animated features, such as UP, American Dad, Family Guy or South Park? If we can't figure this out, and few marketers can distinguish between 11 and 12 year olds and 13 year olds for the purposes or advertising campaigns and marketing, how will a site operator be able to do so?

The addition of "music" and "animated characters" and even celebrity spokespeople may be more effective when seeking sites for younger children. If Big Bird is used on a site, or Blues Clues' Steve, we can assume it is directed at children (or their parents for their children). The same is true with the Disney Princesses. But these are already covered under the non-exclusive list of enumerators. This applies equally to music, as well. Cute jingles, Barney songs, sing-a-longs can help distinguish a site for younger children. But they tend to be more obvious.

Applying "music, "animated characters" and the presence or use of celebrities for tween sites will only cause confusion. How do operators struggle to determine whether a particular celebrity "appeals" to children. We believe the standard should be unchanged so that operators can understand when they are considered to be directing themselves towards children and purposely avail themselves of that market rather than whether children find a celebrity appealing or not. Directed at children must be a decision made by the site, not the preteens themselves. Those acting in good faith are obvious, as are those trying to hide behind a "no users under thirteen" age-gating intended to be ignored by preteens.

d) Support for the internal operations of the Web site or online service.

In its effort of clarify the definition of "disclosure" the FTC proposes new language that explains what "support for the internal operations" means. We believe the definition is confusing for two reasons.

- First, the qualifier that an activity must be "necessary" is unclear and will introduce confusion to operators who cannot be expected to evaluate whether a particular activity is necessary to maintain the functionality of their site. Is this an objective or subjective test? Determined in hindsight, or reasonably anticipated or commercially necessary, or something else?
- Second, the definition does not expressly include activities that can be used to increase the safety of a site or its users. For example, disclosing an IP address to law enforcement in exigent circumstances should logically be permitted, but under the proposed changes may not be. This should be clarified, as should all instances when information may be shared or used to protect their site, the child, the public or third parties

(subject to notice to parents about using information for the safety of a child that currently exists under COPPA's exceptions).

The proposed definition of "Support for the internal operations of the Web site or online service" narrows the term "internal operations" to those activities necessary to: (i) "maintain the technical functioning of the Web site or online service"; (ii) "protect security or integrity of the Web site or online service"; and (iii) "to fulfill a request from a child".

We feel the revised definition may not take into account legitimate business arrangements that exist between related corporate or business entities or third party service providers which support or provide functionality to a children's online property, such as those that administer contests and deliver prizes to winners, those that monitor chat, etc. However, we are mindful and supportive of the policy that seeks to control behavioral advertising and profiling for advertising purposes. As a result, we would recommend the definition be clarified so that legitimate business relationships may exist and not be captured by the definition, but still have the definition capture and restrict behavioral advertising and profiling for advertising purposes. The following is provided as a sample revision:

> "Support for the internal operations of the Web site or online service means those activities necessary to maintain the technical functioning of the Web site or online service, to protect the security or integrity of the Web site or online service, to fulfill a request of a child as permitted by §312.5(c)(3) and (4), *or to deliver content or support services required by the Web site or online service operator, provided that the information collected for these activities is not used for user profiling for advertising purposes or behavioral advertising targeted to children."*

Unintended Consequences to Child Safety and Welfare - We recognize and appreciate the effort that went into developing the Proposed Rule modifications. One unintended consequence of some of these proposed changes, however, is making the preteens less safe.

Preventing the collection of as many types of information may sound appealing and be effective when advertisers are the ones form which the children are to be protected. But it doesn't work as well when we are protecting them from predatorial adults, each other and protecting the site itself. Many other filed comments have centered on operability of the site and technology. But none of them dealt with the safety of the child.

The FTC has previously recognized the need for sites to keep themselves secure and children safe. COPPA itself, as previously mentioned, came from a dual prong need – protecting children from predatorial marketing and from predatorial adults. However, some of the proposed changes might inadvertently restrict a site's ability to defend itself from denial of service attacks, malware, and from protecting children from themselves and others. Without evidence of real abuses, we recommend treading lightly in areas that may curtail a site's ability to protect preteens. They are sometimes the only one to know if a child is at risk to themselves, others or from third parties. Children often confide their secrets to animated characters or feedback forms. These can surprising include suicidal thoughts or parental abuse. Being able to identifying these children and reach their parents (when appropriate) may save lives.

In Conclusion – Taking a direct approach:

We believe that most of the problematic aspects of the proposed revisions are based on policies related to behavioral profiling and advertising concerns. Although we agree with these underlying policies, we believe that the Rule changes, as proposed, do not achieve this policy objective in an effective and undisruptive fashion. Rather than expanding critical definitions, such as personal information and collecting, and coupling them with exemptions (all of which we find confusing and unclear and will in practice result in unintended and undesired consequences), we recommend behavioral advertising and profiling without parental consent be specifically

prohibited. This could be done with a stand-alone prohibition provision, or by carving out this use of information from existing permitted activities.

At the end of the day, whether it be via the use of screen names, cookies, persistent identifiers, etc., it is the use of information, for behavioral profiling and advertising that is problematic and should be specifically curtailed. Taking this direct approach will provide simplicity and clarity, will avoid unintended consequences, and will keep this use of information in check in the future, regardless of ways in which technologies, advertising practices and methodologies evolve and expand.

We have always supported the policy of protecting children's privacy online, and we believe that children should be protected from behavioral profiling and advertising. However, we believe the proposed changes to the Rule should prohibit these uses directly to avoid confusion and unanticipated ramifications, and to permit the Rule to be effective going forward as technology and the advertising industry evolves. We believe the currently proposed changes to definitions have unintended consequences that need to be addressed – either by drafting directly to curb behavioral advertising and profiling which is at the heart of the FTC's proposed changes, or by providing exemptions for valid practices such as inter-functionality between related online properties across all platforms, and business arrangements that are inadvertently implicated by these new definitions.

We strongly urge the FTC to provide for grandfathering for existing online properties in respect of fundamental changes which will significantly impact their business models, and to provide for transition or phase-in periods in order to permit operators to achieve compliance with other changes.

---

[1] Since formation in 1995, the volunteers at WiredSafety (the world's first Internet safety and help group) have been assisting victims of online crimes and abuse, providing education to parents, students and law enforcement and advising Congress, the United Nations, the Home Office, the industry and policymakers worldwide.

[2] WiredTrust offers advice and technology innovations and solutions for the digital industry, 24/7/365 live moderation services to pre-screen for COPPA compliance among other issues and conducts thorough audits of its clients' digital policies and practices.

[3] Since 1994, she had been advising many of the leaders of, and the newcomers to, the children's Internet industry. She, together with Ms. Savitt, was engaged to prepare the ESRB's initial COPPA Safe Harbor application and assist in its approval. Her book, A Parent's Guide to the Internet, (published in 1996) was the first of its kind. Almost 1/3 of the book was dedicated to privacy issues and children. Since then, her books have been translated into 12 languages, adapted or originally written for Singapore, China, England and Spain and cited by hundreds of other authors and researchers. Ms. Aftab is also actively involved in child safety issues, and is the recipient of both the 2011 FBI Director's Award and the 2011 Canadian RCMP Child Recovery Award . Several of the comments contained herein reflect her expertise in child protection and her commitment to making sure that the Internet industry does its part in helping keep children safe from adults, each other (cyberbullying) and protecting all stakeholders from attacks launched by young people against the site, as well. She also designed and built the Girl Scout's Internet safety program, LMK.GirlScouts.org, and is very engaged in providing educational programs for consumers, young people and schools, as well.
Ms. Aftab sits as one of five members of Facebook's International Safety Advisory Board and MTV's digital abuse advisory board (athinline.org). She also was appointed to the Harvard Berkman Center's Internet Safety Technology Task Force (the "ISTTF") and to the NTIA's Online Safety Technical Working Group to advise Congress on digital child safety issues. Vinton Cerf appointed her to the Internet Society's Societal Steering Committee and she was elected to head the Internet Society's Societal Task Force. As the first Chair of McAfee's Consumer Advisory Board, she helped raise awareness of consumers' need to understand privacy and security. Ms. Aftab was a member of TRUSTe's board of directors and the Ad Council's Advisory Board for many years. (For more information, visit aftab.com)

[4] Ms. Savitt also filed a comment to the Proposed COPPA Rules. The undersigned join in and support all of Ms. Savitt's points, some of which are reiterated herein.

[5] FTC Proposal, p. 59819, footnote 151, refers to our earlier comments and states "See WiredSafety.org (comment 68), at 21 (''We all assumed [email plus] 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'')."

[6] "Eliminating E-Mail Plus will make it much more difficult for sweepstakes and contest operators to obtain reasonable assurances that parents do not object to the collection of a mailing address necessary to notify a child that she has won."

> [7] The proposed revisions [of the COPPA Rule] could be read as calling into question the FTC's current position that the one-time use exception of Section 312.5(c)(2) permits collection of online contact information to contact a parent to obtain a mailing address to send a prize that a child has won or to facilitate sending an e-card initiated by a child, in both cases where no other use of that information is used. This is due to a very slight wording change. The PMA assumes that the FTC did not intend to change its position on these uses as a result of the wording change and seeks clarification that these uses remain under the one-time use exception.
>
> Operators of sweepstakes, contests and promotions rely on the one-time use exception to efficiently obtain a mailing address from a parent to send premiums or prizes to children. In its October 7, 2008 FAQs about the COPPA Rule (the "FAQ"), the Commission specifically approved of this approach:
>
> "42. I want to have a contest on my site. Can I use the one-time contact exception to parental consent? ….If you wish to collect any information from children online beyond an email address in connection with contest entries – such as collecting a winner's home address to mail a prize – you must provide parents with direct notice and affirmatively obtain prior parental consent, as you would for other types of personal information collection beyond an email address. If you do need to obtain a mailing address and wish to stay within the one-time exception, you may ask the child to provide his parent's email address so that the parent may be notified if the child wins the contest. In the prize notification email, you can ask the parent to provide the home mailing address to ship the prize, or invite the parent to call a telephone number to provide the mailing information." [emphasis added] The key provision of the COPPA Rule was Section 312.5(c)(2), which is now proposed to be Section 312.5(c)(3). Old Section 312.5(c)(2) provided the exception "where the operator collects OCI [online contact information] from a child for the sole purpose of responding directly on a one-time basis to a specific request from the child, and where such info is not used to recontact the child and is deleted by the operator from its records." (Emphasis added.) Proposed new Section 312.5(c)(3) would provide the exception "where the sole purpose of collecting a child's OCI [where (c)(2) permits collecting the parent's] is to respond directly on a one-time basis, is a specific request from the child, and where such info is not used to recontact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records after responding to the child's request." (Emphasis added.) A promotions operator needs the parent's e-mail, not the child's, to contact the parent and get the mailing address for prize fulfillment to stay within the one-time use exception and avoid having to obtain verified parental consent. The changed language prevents this, and thus FAQ #42 seems to lose its basis of support. Furthermore, the current scheme furthers the maxim that operators should only collect the information necessary to enable children to participate in an activity. If 100,000 children enter a contest or sweepstakes, but only five will win prizes that will be mailed to them, it need not collect physical addresses from all (and thus require all to obtain verified parental consent as a condition of entering). And, waiting until winners are selected to inform them that they must obtain verified parental consent to receive the prize is likely to result in an inability to obtain such consent from some resulting in prizes going unawarded (a regulatory problem in some jurisdictions) or a more complex selection, awarding and fulfillment method requiring the need for selection of runners up. In either event, the same additional costs discussed above will apply and we have members that have indicated that they would scale back on offerings directed to children should such change be adopted.

Quoting PMA's Comment dated December 23, 2011.

[8] Headbone (with more than 300,000 registered users), Freezone (with approximately 250,000 users), Bonus and SurfMonkey were among those which didn't survive. They were online household tween brands in the pre-COPPA days of the Internet.

[9] Parry Aftab has testified before Congress several times about the cost and difficulty in obtaining verified parental consent when financial transactions were not otherwise involved (purchases of access, points, subscriptions or products). See, for example: http://aftab.com/index.php?page=congressional-testimony; http://www.ftc.gov/os/comments/copparulerev2010/547597-00084-54997.pdf.

[10] The only time either Parry Aftab or WiredSafety volunteers received inquiries from parents seeking contact information to make website inquiries was for big social networks and online services that did not permit preteen use. Out of the hundreds of thousands of inquiries received over the last ten years, none related to confusion over who or how to contact on a COPPA-compliant site, network, virtual world or game.

[11] Quoting from Nancy Savitt's comment:

> Email plus has resulted in websites that shun communication tools while offering enticing content to young users. If there is no differential in the consent mechanism used, there will no incentive to exclude communication tools for children. In for a penny, in for a pound, as the saying goes.
>
> When the Rule was originally enacted, the Commission recognized that the other consent mechanisms were more expensive and onerous (see, e.g., 64 Fed. Reg. at 59901 ("In determining what is a 'reasonable effort' under the COPPA, the Commission believes it is also appropriate to balance the costs imposed by a method against the risks associated with the intended uses of the information collected.")). Opening an email is less time-consuming than having a trained employee take consents over the phone, examine a fax or snail mail form for how the signature looks, etc. That equation has not changed in the past dozen years. The Commission's estimate of time to comply with this rule change – 60 hours, to change the notices and technically implement the new consent mechanism, and the focus on "lawyers" and "computer programmers" (76 Fed. Reg. 59804, 59827) – takes no account of the extra manpower that will be needed to carry through the consent process on a day-to-day basis as compared to email plus, not to mention the costs of getting upgraded consent from the parents of all current users.
>
> Email plus is also easier for the parent (or a school functioning for the parent), who does not have to engage in a monetary transaction; print and mail or scan a form; photo-copy a drivers' license; or make a phone call. This ease is commensurate with the lower risk entailed in websites that shun communication tools and thus the risk of public disclosure of personal information. Nothing has changed in this regard since the Commission reached that same conclusion in 1999. 64 Fed. Reg. at 59902 ("[U]nder the second prong of the inquiry, the Commission believes that, until reliable electronic methods of verification become more available and affordable, these methods should be required only when obtaining consent for uses of information that pose the greatest risks to children.").

[12] See, Jules Polonetsky and Christopher Wolf, the Future of Privacy Forum COPPA Proposed Rule comment submitted December 22, 2011

[13] Metadata and Encoded Evidence (taken from Parry Aftab's Cyberbullying Investigation Guide for Schools, written for the StopCyberbullying Toolkit (stopcyberbullying.org))

> Digital photographs often hold vast amounts of metadata. The digital cameras themselves create metadata, and the photographer can also create metadata to attach to the photographic file. The more sophisticated the camera used to take the picture, the greater the amount of the metadata available. This could include the name of the photographer, make and model of the camera used, hidden comments made the user, keywords used to help the photographer find the file, time and date, location, or the description and origin of the photograph. This information is stored in Exchange Information File Format (EXIF), and is even accessible through Windows Explorer. Id. Windows users can also edit the description and origin categories in the metadata. (However, computer forensics could reveal such edits by looking at the system metadata of the operating system or application used to make the changes.)
>
> Metadata is information stored with digital content or communications. There are three basic categories of metadata: substantive, system, and embedded. Substantive metadata is metadata created by the application used by the user, and is usually embedded within the application itself. This category of metadata often shows information about the modification or editing of a document or file. When cyberbullying occurs and there are allegations that the document or image used in the cyberbullying had been doctored or changed substantive metadata could allow the investigator to discover whether files have been altered by another party.
>
> System metadata is created by the user, the system or network being used. This metadata includes programmed information about the author, technical information about the author's device, possibly the location, and the date

and time of the publishing or modification of information. This metadata will help identify the device used in creating the content, and depending on the accuracy of any programmed settings, the owner, date, location and time the content was created. It can often help determine the "ground zero" of a cyberbullying, harassment or sexting campaign.

Embedded metadata consists of the content, data, text, or other information that a user inputs his or herself, but which is not typically visible when viewing the native file. Examples of this include spreadsheet formulas, and internally or externally linked files, such as hyperlinks or sound files. This is often used to help mask the real cyberbullying. Linking an innocent-appearing image to a rumor-mongering Facebook post or nastier manipulated images makes it easier to launch a cyberbullying public campaign without being obvious to school authorities or other adults.

[14] iPhone and iPad, as well as more recent iTouches, Nintendo DS with photo capability and Photoshop, among others, provide these tools which are widely used and enjoyed by preteens to distort their image for fun.

[15] There have been instances where young people have been cyberbullied for vocal performances and mocked online for perceived lack of talent, but this is not a COPPA-related risk.