Parry Aftab, Esq.

September 24, 2012

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

Via Online Submission

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

Dear Secretary Clark:

I am an Internet privacy and security lawyer, the Managing Director of WiredTrust, an Internet risk management consulting firm ("WiredTrust"), and Executive Director of WiredSafety, the world's oldest Internet safety group ("WiredSafety"). I am filing this Comment in my individual capacity and in further support of the Comment submitted jointly by WiredTrust and WiredSafety.

I appreciate the willingness of the FTC to solicit comments from the public, advocacy groups and policy and industry leaders to the Supplemental Notice of Proposed Rulemaking (the "SNPRM").[1]

Together with WiredSafety and WiredTrust, I would like to recognize the hard work of FTC staff and executives and their continued commitment to engage all stakeholders and remain accessible over the years. I especially appreciate the time certain FTC Staff members, especially Mamie Kresses and Phyllis Marcus, have devoted to my inquiries and thoughts over the years. These discussions have been invaluable and I value this access. I have been honored to participate over the years in many briefings and had been actively engaged in the drafting of COPPA in 1998.

I previously filed comments on the Commission's Notice of Proposed Rulemaking published on September 27, 2011 (the "2011 NPRM") jointly with WiredTrust and WiredSafety, many points of which

[1] Federal Trade Commission, Supplemental Notice of Proposed Rulemaking and Request for Comment, Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643 (Aug. 6, 2012) (hereinafter "SNPRM").

were referenced by the Commission in the SNPRM. Those comments are renewed herein, to the extent they are relevant.

While I am not a stranger to the FTC and Congressional Representatives, it may be helpful to put my comments into perspective once again. I represent and have represented most of the industry leaders over the years. I am both a member of Facebook's Safety Advisory Board and MTV's a Thin Line Advisory Board. I also work closely with law enforcement agencies to help protect all users, especially children, from criminal activities online.

My comments are designed to be more practical than those of WiredTrust and WiredSafety. They come from the trenches of representing children's industry players (large and small), game operators and device manufacturers. I will point out when things will and won't work, to the extent I have insight. I also served on the Internet Safety Technology Task Force at the Harvard at the behest of 49 of the state Attorney General, examining age-verification technologies for children. I have served on other governmental advisory boards in the US and internationally, most directed at children's safety and privacy and industry best practices. Last year I receive both the FBI Directors Award and the RCMP's Child Recovery Award for my work in protecting children online.

My comments to the SNPRM include discussions of the following proposed changes:

- The Effect of these Proposed Changes on the Recovering Kids Internet Industry
- Co-Operator/Plug-In Provider Liability
- Expansion of the Definition of Web sites and Services Directed at Children
- COPPA Verifiable Consent Platforms
- COPPA's Internal Operations Exception

Contents

The "Devil is in the Details" 3

The Effect on the Recovering Industry: 3

Co-Operator/Plug-In Provider Liability: 4

Expansion of the Definition of Web sites and Services Directed at Children: 5

The Internal Operations Exception and Platform Consent Mechanisms for Verifiable Parental Consent: 7

The "Devil is in the Details"

While the proposed changes may appear on their face to provide a reasonable approach to resolving issues with industry practices and children's privacy, security and safety, they may create more confusion and less protection than intended. They also carry substantial unintended negative consequences.

The Effect on the Recovering Industry:

When COPPA was first launched, in April 2000, it was on the tails of the Internet crash of March 2000. The children's Internet industry was devastated. Advertising revenue was not paying off and this pre-dated the subscriber model introduced successfully by Disney's Club Penguin. We lost a vast percentage of the midlevel children's sites and services, such as Headbone, SurfMonkey, Bonus (a later casualty) and others. The industry entertainment leaders (such as Viacom, Disney and Fox) dominated this newly-reduced member field.

It took years for the smaller and midlevel sites and services to begin to recover. Now, they are once again becoming known for their innovative approaches, their mobile and new device apps and their ability to engage, educate and entertain preteens.

I fear that the proposed changes, while well-meaning, could have the same devastating effect on the new digital innovators for children. In addition to being a child privacy and safety advocate, I advise many of the longtime leaders in the children's space, as well as many of the newcomers. I was coined the "Kids Internet Lawyer" in 2000 because of the number of child-related clients I advised.

Over the years, I have learned a lot, often the hard way. When we seek to protect children's privacy, safety and security, we must also try and strike a balance with the need for new sites and services to address the growing hunger for quality digital offerings for preteens in a reasonable and realistic way including adoption of all best practices. We have choices:

- We can make the digital world entirely safe for children by excluding them entirely. But that is not the FTC's intention nor mine. I have been quoted often for my response on the greatest risk children face online. My response has not changed in 18 years: "The greatest single risk our children face online is being denied access. We have solutions for everything else."
- We can excessively regulate the industry to require bulletproof protections, blocks and pre-monitoring of all children's activities. But that is not the FTC's intention nor mine. It would leave us with no industry at all (aside from the bad players who don't care about privacy, safety or security and those which must take shortcuts in safety because of the added cost and time demands of these excessive regulations).
- Or, we can require that parents must review and approve everything their children do on all digital devices before their children can access even the valuable, educational and appropriate entertaining sites and services. But that is not the FTC's intention nor mine. Parents have a tough job already without being hammered with hundreds of requests for their review and

consent to all their children's activities online, on the mobile and on game devices. They will reject all requests (which they did for years following COPPA's initial adoption, refusing to provide credit card details or offline contact information) or approve everything like deer caught in the headlights.

We must take care that regulations designed to protect children don't have the unintended effect of denying them reasonable access or chill quality content, interactivity and communication innovations that can enrich their lives and learning. I fear that most of these proposals (as proposed) will do just that. We will be denying children access unnecessarily, requiring them to lie further about their age, over-burdening parents or killing valuable digital choices because of the bad actors or clueless ones.

Co-Operator/Plug-In Provider Liability:

The FTC seeks to require that plug-in providers are subject to COPPA merely by the nature of their being adopted by a child-directed site or service. I believe this is objectionable. In this, I adopt CDT's comments, referenced in the SNPRM.[2] It is unfair to burden a site or service merely because a third-party chose to utilize their product or services. A site's or service's intentional actions should make them subject to or not subject to COPPA, not a third party's actions.

This is closely linked to the expanded "knowledge" test. These providers do not target the adoption sites or services, they merely provide a function that is often expected by users on interactive websites. They don't prescreen them. They don't, in most cases, categorize them, either.

If, however, the plug-in or software provider promotes their product directly to a category of child-directed sites or services, intending to access that market, they are (in such cases) no different from other child-directed websites or services and COPPA already applies.

If their plug-ins are available at child-directed websites or services, does this not make them a child-directed site or services for all purposes? If Sesame Workshop adds a "like" button to its pages, does that make Facebook a child-directed site because they can reasonably infer that a Sesame Workshop users is under 13? I don't think so.

I have been practicing digital privacy and security law since the dawn of the Web. And I don't think I could draw a reasonable inference on many sites and services unless investigating them. How can we expect most plug-in providers to do this? And do we even want them to?

Where there may be sense in requiring that certain plug-in providers apply the "reason to know test" to whether their involvement in a site or service requires their COPPA compliance (discussed below), in most cases it will require more manpower, professional advice and costs to providers than is warranted. Many plug-in providers have no direct financial benefit from children's plug-in use.

Instead of using a broad brush to color all plug-in providers, perhaps we should look to the business model used by each provider and how much they know and want to know about their preteen users.

[2] SNPRM footnote 16, referenced in the text.

Advertising networks, data-mining companies and others seeking to gather special databases of users, including preteens (perhaps classifying them are merely game-players), make their living knowing their users. They understand the likelihood of preteen users and financially benefit from that information. In this case, requiring them to make reasonable inferences makes sense. They benefit from preteens, can make a reasonable inference that the users are preteens (and promise their customers or owners that they have done so effectively) and should be required to jump through COPPA hoops. It's one of the costs of their doing business the way they do it.

Unlike this category of plug-in provider, however, those such as Facebook with its "like" button have no interest in collecting preteen user information. To use the "like" feature, the user must have a Facebook account and to do so, must be age-gated. Twitter "shares" fall into this category, as do many blog sites, Yahoo! and Google's GooglePlus. Other than age-gating, we should not want them to draw inferences, reasonable or otherwise. These types of plug-ins are simply allowing users to do what they expect they can do when old enough, share their likes, delights and their ideas. It's Web 2.0 connectivity and community. It stops at their age-gated door, however.

In our joint NPRM comment (sited by the FTC in several instances in its SNPRM), we recommended that use be given a higher priority than merely limiting collection. It allowed for fewer work-arounds and gets to the essence of COPPA. Here, that approach works particularly well. If plug-in providers sort the data they collect or can access, intentionally to classify preteens holding them accountable for the information they collect and access from "inferred" preteens makes sense. If they don't, merely providing "like" or similar features to pages, profiles or services of all types, they should not be classified as COPPA-covered providers for this purpose.

Expansion of the Definition of Web sites and Services Directed at Children:

Expanding the definition of Web sites or services directed to children and those which know that they are collecting information from children (under the existing COPPA tests) to include Web sites or services which "[have] reason to know" is particularly problematic.

From its inception, COPPA was based on the premise that a site knew if it was "directed to children" or would have to have actual knowledge that it was collecting information from children (which included allowing children to share PII with others using the Website or service). Attempts to enlarge the "actual knowledge" test to include implied or constructive knowledge were rejected regularly. (See Becky Burr's and my comments from the FTC 2010 Privacy Panels.)

The FTC argues that "reason to know does not impose a duty to ascertain unknown facts".[3] It suggests that it merely requires that a person draw a reasonable inference from information they do have.[4] While this sounds reasonable, how would it be put into practice? Do we want these sites or services combining data they may have access to in determining the nature and demographics of a site or service? COPPA seeks to discourage cross-site or service tracking. This might do the reverse.

[3] SNPRM footnote 18.
[4] Id.

In the time of data collection, projections and analysis, what does a reasonable inference involve? If they may a reasonable inference and are wrong, are children refused access? Are they liable for drawing the wrong reasonable inference? How many new profiles will these providers now collect to meet the reasonable inference/reason to know test?

Other proposed provisions are problematic as well. They are undefined, subjective tests that will make it impossible for operators to determine when they are "Operators" for the purposes of COPPA. The practicalities of sites or services legitimately directed at young teens which have an unintended influx of preteens seeking teen-directed sites and services are real. The FTC determined not to extend the age of COPPA-covered minors beyond twelve. Yet, by drawing in sites and services not intended for preteens which have a larger percentage than expected of preteen unsolicited users, we are doing just that. Now all teen sites run the risk of being classified as an "Operator" under COPPA 2.0.

Telling the difference between a 12 year old and a 13 year old online is impossible. And how a site or service should calculate the percentage of preteens to the general population is unclear. Even the US Census Bureau does not break down the number of preteens within the US population. It categorizes birth through and including 13 year olds. If the US Census Bureau cannot provide the percentage of preteens in the US population, how should a website or service?

It is clear that the FTC wants to close existing gaps in COPPA that allow bad faith operators to avoid asking for ages and pretending they have no knowledge of preteen users, or pretending that they are directed at teens or the general population when they know otherwise. The "wink/wink/nod/nod" practice of "don't ask and don't have to comply is something we all want to stop. But, I respectfully submit, this is not the way to do that.

The Commission has indicated that they have not taken action against a site or service when they were in good faith targeting teens and not preteens. They explained that this was due to the burden it imposed on child-friendly mixed audience sites. They also were concerned about the point made by Disney, and others, that child-friendly mixed audience sites are often required to use a one-size-fits-all approach, either don't ask age at all or age-gate everyone. Disney and others have always been able to age-gate all users and treat them accordingly.

If sites should age-gate because they are directed at preteens, they should age-gate. COPPA already requires that. But under this proposal, most teen sites will be forced to age-gate to avoid being held in violation of COPPA. Voluntary age-gating, requisite notice and consent mechanisms are fine. But mandatory and unnecessary broadening of COPPA to all child-friendly general audience sites is not what COPPA was designed to do.

The original definition of directed at children was flexible and effective. We could look to what the sites or services told their advertisers (as in the case of Xanga.com), or the kinds of advertising appearing on the site, or the offline targeted market of the entity owning or controlling the site or service. By looking at site practices, we can distinguish the bad players or clueless ones from the honest ones.

I fear that these vague measurements and standards will be burdensome, overbroad and confusing. They are subjective, vague and will be difficult, if not impossible, to measure and the evaluation may change from time to time based on promotions that attract a younger audience for a period of time.

The Internal Operations Exception and Platform Consent Mechanisms for Verifiable Parental Consent:

Perhaps the most positive result of the COPPA 2.0 review process has been the renewed interest and activity in the collective consent platform space. In 2001 I first proposed the creation of a "Central Site Registry." The former FTC Staffers involved with the creation of COPPA worked with us to help find a working model. It was going to be run by a non-profit and provide verifiable parental consent on behalf of authenticated parents for websites and services that met certain disclosed criteria. It was a proxy model, more expansive than the app consent models being discussed now. Parents would set approved criteria and the registry would match site standards to the consents. New sites could seek approval and the proxy consent when released. And parents could reject sites specifically or tailor their consent under certain circumstances. Sites would ping the Registry to confirm the applicable consent and parents would be sent notice when their child requested access to a new site within the Registry. Sadly, the CSR was never released as other issues became more critical in the child safety space and the World Trade Center attacks consumed our online protection staffing. But the planning, collaboration and thinking still applies.

Facebook, Apple and others are in prime positions to verify parents for digital COPPA consents, using PIN numbers for future communications under the requisite COPPA authentication standards or other accepted models. Parents can click the individual box or select all to approve apps and third party technologies that meet agreed upon and disclosed standards. The sites, apps and services would have to provide contact information, adequate notice, compliant policies and other COPPA compliance steps, but would not longer have to "go-it-alone." Verifiable parental consent will be within reach of even the smallest operators at minimal or no cost.

This is promising. And possible. But the platform, collaborative consent model involves the collection and use of information by the platform providers. And they will need to be clear on liability for non-compliant apps that promise compliance. They cannot and will not conduct due diligence or independent inquiries of information provided about app practices and policies. And they will need to collect and use information to maintain the consent platform that should be classified as "internal operations" data.

The "internal operations" exemption has been overtaxed in recent years. It was designed for site security and security of operations (child security purposes require notice to parents), backend operations and to allow the site to deliver its site. I was heavily involved in its drafting. We expected that this exemption would be further clarified over the years, but little attention has been paid to what a site can consider internal operations, other than the obvious. Should it include optimization of flow and usage? Probably. Should it include first party customized advertising? Maybe, unless personal information is being collected and used that would otherwise require email plus. With email plus being

potentially retired, should this be something that becomes internal operational data or require verifiable parental consent?

Entities that offer plug-ins for third parties have the need to monitor them. Is the information collected internal?

Fifteen years after being signed into law, it is time to address the realities of backend operational data in helping sites understand their users, their patterns, needs and desires. It is crucial to keeping sexual exploitation and other crimes and abuses under control. It helps track criminals, threats and stalkers. It helps the site run more efficiently and smoothly, and better address the needs of its stakeholders.

I suggest that the FTC hold briefings on this issue, allowing for commentary and contributions in a less formal setting, to help bring certainty and clarity to this evolving question. Especially as central consent mechanisms are being developed, the ability to use user information to enable better COPPA compliance and parent engagement is worth it.

I adopt the formal comments of WiredTrust and WiredSafety and incorporate them herein, in their entirety. I have also attached Exhibit A, US Census Bureau data effective 2011 of the general population by age, which is incorporated herein. To the extent my comments align with those of the Future of Privacy Forum comments, and those of Facebook, CDT and Disney, I have adopted and provide my support for those as well.

Please feel free to contact me with any questions or clarifications I can address. Again, thank you for caring so deeply about the privacy and safety of children. It is one more item on which we can always agree.

Very truly yours,

PARRY AFTAB,ESQ.