July 9, 2010

By Electronic Filing

Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
Room H-135 (Annex E)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: COPPA Rule Review, P104503

Dear Secretary Clark:

As an FTC approved safe harbor under the Children's Online Privacy Protection Act (COPPA) Privo appreciates the opportunity to provide brief comments to the FTC as it undertakes a review of the Commission's Rule implementing COPPA.

We are pleased that the FTC has recognized that not only have new online services emerged for the children's demographic that are specifically protected by COPPA but that some of those same services that are intended for children 13 and above are undeniably attracting and interacting with children who should otherwise be afforded COPPA protections. Additionally, it seems clear from the request for comments and the COPPA workshop held in June 2010 that the FTC recognizes that new parental consent methods are needed, already available and/or possibly contemplated and that the methods outlined in the Rule more than 10 years ago were never intended to be an all inclusive list of reliable methods. Methods that have been specifically called out in the Rule are believed by many to be the only methods allowed. That belief is not correct and stifles innovation. We hope that the FTC will make their position clear in its review. Many might not be aware that the FTC in its 2005 COPPA review stated "Infomediary services act as middlemen in obtaining verifiable parental consent for Web sites and can offer options such as driver's license and social security number verification".* *[* FEDERAL TRADE COMMISSION 16 CFR Part 312]* These "options" or verification methods by infomediaries were not intended to be all inclusive, set in stone or rigid in their implementation, nor are they perfect. All organizations that are directed to or attract a significant percentage of U13 along with infomediaries must strive to comply with the General Standard for obtaining "verifiable" consent.

Fact: Infomediaries already exist that allow a parent to create a single credential and use that verified credential (from email plus to more reliable verified identity) to permission children's use of online services and participation in marketing initiatives through turn-key registration solutions and through discrete web services. The incremental cost of each reliable verification method along a sliding scale can range from $.01 – $1.00 per transaction.

Thought: COPPA should not be seen as a ban on marketing to children under 13 (U13) but instead the parent should have a say. COPPA should be seen as a set of mandated guidelines supported by best practices that allows for the informed consent of a parent for their children's disclosure of personally identifiable information (PII).

Privacy Vaults Online, Inc., d/b/a Privo
8229 Boone Blvd., Suite 410 ■ Vienna, VA 22182
http://www.privo.com email: info@privo.com PH: 703.569.0504 FX: 703.783.8752

Request: We need to fully open the door and recognize that new processes or innovations need not obtain specific FTC approval but rather the FTC should encourage industry to create, adopt and deliver methodologies that make a reasonable effort to meet the General Standard which says that "operators must take reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent".

Vantage Point: As an FTC approved safe harbor we speak from a unique vantage point. Not only have we consulted and certified dozens of organizations for compliance with COPPA but we ourselves have built and deployed technology services to enable child, adult and teacher initiated registration, identity verification along a sliding scale and parental consent management for opt-in or opt-out services. In our opinion, industry is desperate for clarification, refinement and direction as it relates to the job of actually complying with COPPA at a tactical and a "in the spirit of" level.

Suggestion: To our knowledge there is currently no formal procedure for considering or approving additional reliable methods under COPPA. Perhaps the FTC could specifically state that if a safe harbor certifies an operator under COPPA and that operator is using an innovative methodology not specifically called out by the FTC or the Rule then the Commission will deem the online operator to be compliant. If the FTC or another safe harbor is not comfortable with a method approved by a safe harbor then the FTC can take the issue up with the safe harbor. This would likely spur innovation at the site operator or online service level to attempt reasonable efforts given the specific needs and risk of their online property or service. Over time verifiable parental consent methods will come and go as industry makes reasonable efforts to adopt methods that achieve the goal of obtaining verifiable parental consent. However, until the FTC makes it clear that industry must find and adopt reasonable methods the bar will remain low and stuck in a time warp from 10 years ago.

Obvious to Most: U13 kids are often being given no choice but to lie about their ages because the sites they are attracted to are not willing or not interested in obtaining parents consent for children under 13 (U13). Our experience is that parents are for the most part unaware of COPPA and its intended benefits and are under extreme pressure by their children's desire to participate with friends and other family members online. Therefore, at times parents find themselves agreeing to circumvent terms of service and unknowingly COPPA by allowing their child to age up in order to obtain access to popular social networking sites and online supported phone apps for their minor children. Would we suggest a parent should be ok being put in that position (it's ok to lie to the operator because I said so) in the offline world?

During the FTC workshop held in June 2010 we learned from Ron Zayas, CEO of eGaurdian that "we went to about 100 different schools, and we matched the parents and the kids to the schools, and we asked the parents, "How many of your kids – "and these are between middle school and elementary – "How many of your kids have a Facebook or a MySpace account?" And almost universally, the parents said, "My children don't." And then we matched it up with their actual children, and we asked them, "How many of you have --?" And about 60% to 70% of them did. So, I don't know if it's so much "Are parents complaining that they're not getting asked?" "or that they even know it exists would be the better question".

A recent study of 7-10 year olds in the UK found that 3 out of the top 10 games that they play are Facebook games. This research by Dubit as published in the KZERO.co.uk blog (April 2010) could reasonably be extrapolated to US kids.

http://www.kzero.co.uk/blog/wp-content/uploads/2010/04/dubit-uk-all.002.jpg

Suggestion: Sites that have general knowledge that a significant portion of the protected U13 demographic is using their service under false ages should be required to demonstrate that they are using reasonable methods in light of available technology to ensure the children U13 are not using these services without parental consent. This means the site that implements neutral age screening would not simply rely on children to tell the truth. If a child identifies themselves as U13 then the operator has a choice to both allow the registration and process the proper level of consent or decline registration. If an online site/service's terms of service do not allow for participation by a minor then the site operator should retain for a reasonable period of time the important unique identifier of email and/or cell phone collected during the attempted registration against the DOB in a 1-way hash (a 1-way hash provides an encrypted way to look up and compare the information but does not store the information as retrievable PII). This would allow the site to mitigate the chance of the U13 re-registering to the site. Additionally if the site truly doesn't want U13 then the site operator could listen for notice or ping an identity service for information that might provide the site with enough DOB information to know how to apply its terms of service and also comply with COPPA.

Point of View: Parents who are helping kids circumvent the system may be doing so because many of the popular sites that they are otherwise okay with are not providing an opportunity to tell the truth and provide consent. In our experience, when provided, parents will use tools which help protect their child online. Consequently, we take issue with a statement provided by Dana Boyd, Urs Gasser and John Palfrey, principal investigators of the Youth and Media Policy Working Group Initiative at Harvard's Berkman Center for Internet and Society, which was provided to the Subcommittee on Consumer Protection, Product Safety, and Insurance of the U.S. Senate Committee on Commerce, Science, and Transportation on April 29, 2010 ("Berkman Center Statement"). That statement reads in pertinent part:

> "While gaining parental consent is clearly desirable and crucial for small children on websites where they are sharing information about themselves, it is also important to highlight the ways in which this backfires. Parents who are already engaged know what services their children are using online and are contributing to their efforts to circumvent restrictions. Parents who are not already engaged will not become so if forced to confirm participation, and children in such households will find other ways of circumventing restrictions. Forcing parental involvement through website-initiated confirmation is ineffective, both because data show that these restrictions are circumvented and because it doesn't actually engage unengaged parents." Statement at page 4.

Children are being put in two categories: 1) children with parents who care and are engaged; and 2) children with parents who don't care and are not and never will engage. It would seem there is at minimum a third category and it is by far the largest, parents who care and don't know how or have not been asked to engage or have been forced to facilitate lying to break the rules of an operator's site.

It is important to note that a child requesting permission from a parent who would not otherwise know about their child's interaction with a particular site operator or their child's interaction with others using

an online service would now have a chance to be educated and become an engaged parent.

Opportunity to Clarify another Point of View: A statement contained in the Berkman Center Statement that purports to identify a particular shortcoming of COPPA:

> "We should also highlight that age restrictions without parental consent are doing serious damage to efforts intended to help youth. Any social service – suicide hotlines, eating disorder clinics, or mental health services – that seeks to provide online services must also abide by COPPA. This means that they cannot begin communication with children under the age of 13 without parental consent." Statement at page 4.

We respectfully disagree. First, most social services are run by non-profit organizations which are exempt from complying with COPPA. Second, the online component of the counseling and intervention services provided by most social service agencies is typically minimal. Moreover, even were COPPA is applicable to the services provided online, there is little doubt such services would be subsumed under 16 C.F.R. §312.5(c)(4), the exception permitting collection of a child's information "to the extent reasonably necessary to protect the safety of a child…"

EMAIL PLUS coming or going?

History of Email Plus: Email plus was originally carved out of the Rule as an exception and was thought to be a temporary method to aid industry in compliance. It was intended to be used where the collection of information from a child was only for internal purposes and not to be shared with third parties or to be publicly disclosed. At the time the Rule went into effect it was considered a less-risky, a less-disclosing method of taking personal information. Accordingly it was never intended to be used in situations where personal information could be publicly disclosed.

FTC Question of the COPPA Workshop Panel June 2010: When the FTC did there 2005 five (5) year review of COPPA for Congress they determined that the temporary method of email plus should be made permanent for internal use of data for the foreseeable future. This had the effect of giving industry absolutely no reason to create, innovate, adopt or make use of any other method for the internal use of children's personal data. Five years later the FTC is asking "does email plus provide the same assurance of actually reaching a parent as any of the other – methods in the Rule?" and "do you think that it still makes sense that "email plus" is limited to – internal purposes?"

So what is Email Plus? This simply means to ask the child for his parent email, send the email, require the recipient of the parent email to take an action by clicking a link, then following up with a confirmatory email, phone call or mailing. Of course everyone defaults to the lowest common denominator which is the follow up email. In its current form and use does anyone out there actually think that this provides any assurance that the person providing the consent is the parent or even an adult that could assert they are a parent?

Should Email Plus be Eliminated? Absolutely not. The "plus" should simply get better along a sliding scale use of risk.

How is Email Plus being Used Incorrectly?: Many companies who have filtering in place (either with or without professional moderation) but who cannot ensure parents or government that PII is not being disclosed have adopted email plus to provide both cover under COPPA and an attempt to inform

parents about the companies best practices for child safety. The fact of the matter is that if PII *can* be disclosed then email plus is not meaningful as it relates to COPPA compliance. If PII *can not* be disclosed (i.e. it is identified, stripped and deleted from the servers) then NO method of parental consent is required under COPPA.

The Current Standard: If an operator does not want to incur the hassle, cost, or loss of converting users that might occur with obtaining a reliable method of parental consent then they must provide an experience that would produce disclosure results as if a reasonable person would have identified and deleted from communication obvious PII before the disclosure is made public? Best efforts are defendable but unfortunately this method may not be very scalable.

Request: The FTC should make a determination regarding the use of filtering technology (specifically, what characteristics of the technology must exist in order for the operator to be considered to NOT have collected PII even if the PII becomes public?).

Managing Risk: It's about managing risk for site operators. Could the FTC conclude that social/community/interactive tools and services that implement sophisticated filtering to include … a black list for words and phrases, pre and post human moderation, abuse reporting, education and site accountability can be given the green light to obtain parental consent in a way that is less reliable then what is currently required? If we accept that PII may well indeed be disclosed by the crafty kids (keep in mind these kids could still be the good kids with parents who are engaged and already know what their kids are doing online) then why would we promote or escalate the current version of email plus and conclude that it is good enough for this level of risk? Professional safety experts commented at the COPPA 2010 workshop that you cannot rely on technology alone because kids will indeed try to communicate personal information. That unless a non-fatiguing person read every post there is no way to 100% stop kids from disclosing their personal information and of course that would never scale. If the potential to disclose information still exist then shouldn't we agree that the parent should at least be informed? In order to believe that a parent is being informed shouldn't we do something to try and ascertain if the email address really belongs to the parent. Shouldn't it at least belong to an adult given the median age of parents who have U13 kids?

Why Wouldn't We Create New Scalable and Potentially Global Methods? For instance email plus could be enhanced by a mobile phone or with a name and address that the operator can attempt to match. This would have the benefit of reducing fraud and confirm a person presenting themselves as the parent is at least likely to be an adult? With the existence of identity providers a child could provide an email of an already verified parent or a kid login credential that has an already associated verified parent and have notice delivered to the parent or request email consent based on the verified email. At least this way the site operator could say they did something meaningful to attempt to obtain verifiable parental consent. Of course the presentation of a verified email is much less reliable if there is virtually no proofing or analyzing that goes on to determine who the email belongs to. So the reliability goes hand in hand with the underlying proofing. The goal is to use methods that are reasonable in light of available technology and that the method does as good or better a job of eventually calculating the a the consenter is the parent.

The Debate: What level of parental consent will be good enough if a company uses a bundle of safety measures and mitigates the risk of exposing children's PII and what risk will the lawyers allow their clients to take as it relates to the potential for children to publically disclose their PII? This isn't just about my first and last name or my address or my cell phone. How about the child who is U13

disclosing their Facebook account or IM regardless of whether the parent knows the child has a Facebook account or if the child has their parents nod that having a social networking account on a site that terms of service are 13 and above is ok. As a matter of fact, emerging sites are relying on the fact that users who identify themselves as parents and have a Facebook accounts must indeed be 13 and above. Sites that know they attract kids to their phone or social networking games are relying on the fact that you have to be 13 and above per the app platforms terms of service.

OTHER CONSIDERATIONS

Multiple Use Exception: The answer is, yes operators are misusing the exception to deliver personalized messaging and marketing to kids but never actually obtaining affirmative consent from parents. Many of those operators are still allowing bogus emails to be used and relied upon for having at least provided parents with notice and the right to opt out by not managing bounce backs. Additionally, there are a number of operators who believe that they can add non-PII (example: all or some of the data elements of user name and password, age, gender or zip) to the child's email address or other personal information and not trigger the need for affirmative parental consent. These operators should be stepping up to the current implementation of email plus as a minimum.

Could Schools be a Viable Alternative to Produce Kid/Parent credentials? The answer is yes. This can be accomplished without stepping on FERPA or CIPA and without bringing liability on to the school system. Once the privacy issues are addressed the question is why, why would a school want to get involved. June 10, 2010 Yahoo released findings from an online survey about how parents monitor children's online behavior. The study found that 73% of parents want their child's school to play an active role in teaching kids about online safety and citizenship. Parry Aftab reported at the June 2010 panel she spoke on that "until somebody works on a model that can deal with schools ..." Is there a forward thinking state or school district interested in trailblazing a solution that would better equip and empower their students to be accountable while still respecting their privacy. The issue may indeed be what is the benefit to the school even if the process is low impact?

Privo appreciates the opportunity to provide these comments to assist the Commission with its review of the COPPA Rule. We are committed to protecting children's privacy and safety online, and we look forward to working with the Commission toward this common goal.

Respectfully submitted,

Denise G. Tayloe
President and CEO
Privo
dtayloe@privo.com
703-932-4979