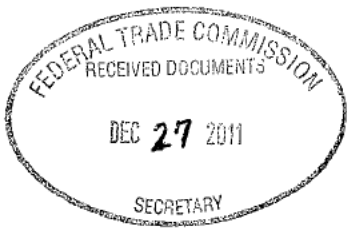
PRIVO
PRIVACY, PERMISSION & TRUST

December 23, 2011

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, 16 CFR Part 312 (Project No. P-104503)

Dear Secretary Clark:

As a Commission approved safe harbor under the Children's Online Privacy Protection Act (COPPA), and a longtime advocate for advancement in the proliferation of informed parent consent, Privo appreciates the opportunity to respond to the Request for Public Comment on the Federal Trade Commission's Proposed Revisions to the COPPA.

Industry, Parents and Kids won when 1) it was made clear that a mobile service or application targeting children is and has been subject to COPPA. Assuming this holds then we do not need separate legislation regarding marketing to children under the age of 13 (U13). The final Rule should provide enough meaningful coverage as it relates to marketing to children through data collection, use and disclosure regardless of the device used by the child. Mobile innovation can now move forward on a level playing field; 2) the age of COPPA protection was held at U13 as it relates to the need for parent consent to collect, use or disclose personal information from a children; 3) the 100% deletion standard was reduced to "all or nearly all" removal of U13 PII which should open up more online services directed to U13; and 4) it was made clear that online operators can feel free to innovate reliable parental consent methods, and that the original methods enumerated by the FTC are not an exhaustive list, that specific approval for new methodologies is not required and that if approval is desired by an organization a process to obtain that approval through the FTC or a Commission approved safe harbor will be in place.

COPPA should not be seen as a ban on marketing to children U13. Instead the marketing practices of the entity should be transparent and parents should be offered a chance to have a say. COPPA is a set of mandated guidelines supported by best practices that allows for the informed consent of a parent for their children's delivery and/or disclosure of personally identifiable information (PII).

Industry, Parents and Kids will lose if the concept of a "sliding scale" is not retained. In 2011 the sliding scale should be defined separately from that of the consent mechanism called email+. Email+ is simply a name for a currently weak method of consent. The concept of a sliding scale for obtaining parent consent has evolved and taken on a very important role. It allows for a graduating, just in time marketing relationship with a U13 child based on the feature or activity being offered; balanced by the level of effort a parent and child are willing to make to join or engage in a service that caters to or simple allows children U13 to participate. Accordingly, the Commission was correct years ago when they were convinced that the collection of U13 personally identifiable information (PII) for the purpose

Privacy Vaults Online, Inc., d/b/a Privo
1651 Old Meadow Lane, Suite 500 ■ McLean, VA 22102
http://www.privo.com email: info@privo.com PH: 703.569.0504 FX: 703.783.8752

of sharing with 3rd parties or making publicly available delivers a higher risk to a child's privacy then the collection of PII to facilitate internal marketing campaigns. A reasonable person would have to agree that there is a distinct difference in internal marketing versus sharing and public disclosure. It also seems reasonable that behavioral tracking falls on the sophisticated side of marketing and therefore, should not be utilized without reliable means of obtaining verifiable parent consent.

Although the FTC's use of sliding scale and email+ are considered one and the same, the reality is that kids engage with marketers and online services along a continuum and the concept of a sliding scale makes practical sense regardless of whether the current implementation of email+ provides reasonable assurance that parent consent has been obtained.

The sliding scale is not the problem. It is actually a very reasonable approach that can be understood by all constituents. The problem is that the method currently used for the PLUS (+) in email+ is too weak. Kids who obtain consent by providing a valid parent email are being properly consented as long as the parent consent is informed consent; kids who do not want to get a parent involved know how easy it is to provide an email that they control. If the parent had to provide verifiable information (not necessarily verified) or take additional steps, rather than simply clicking a link from the notice and request for consent email, then kids and parents might begin to take the consent process more seriously. After all this is what is being proposed in the total elimination of email+.

There are absolutely creative ways to improve the PLUS such that email coupled with other steps may be considered reasonable for internal marketing, but would not rise to the level of protection needed in situations where personal data is shared, tracked or publicly disclosed.

The sliding scale provides a framework to work within as the child's involvement and the site operators' access to market to the child gets more sophisticated. The sliding scale would continue to allow for the following:

- No PII = no parental notice and consent needed;
- Exception use of PII = notice to the parent with the right to opt-out required;
- PII collected for internal marketing efforts only = notice to the parent including a requirement to obtain informed and verifiable NOT verified parental consent;
- PII collected to then share, rent, sell, publicly disclose or combine with other data to track the U13 behavior in conjunction with activities of the child outside of the primary service = notice to the parent including the requirement to obtain verifiable parental consent where the verification of the parent is held to a higher standard.

If we flatten the scale and push all U13 participation that leverages PII to the highest threshold then we will likely have the counter effect of shutting down parent consented legitimate marketing and communication to children. Sites will choose to block registration and rely on actual knowledge or the lack thereof. The other possibility is that sites who are forced to obtain more reliable and costly (.05-1.00 per verification plus the soft cost of lost conversions) consent will feel pressure to make up the compliance cost and loss of conversion by reducing the efforts they are currently making to mitigate the disclosure of U13 PII, safeguards that are currently provided to produce reasonably safe online experiences are costly. Consider that if the site needs to get the most reliable consent for basic internal marketing efforts then a site operator may lose interest in funding some basic safety measures.

There are plenty of PLUS methodologies that could be coupled with email or any online identifier used to contact the parent that would be far better than the current implementation of

email+, would be reasonable for the intended use of internal marketing, but that would not be as reliable as those needed for the most risky use of U13 PII. Example: Child wants to join a fan club that includes a loyalty and/or birthday component, personalized site alerts and offers to further engage. Under the concept of a sliding scale the child could provide a parent email or another online identifier to reach the parent. The parent would have to do more than simply click a link. The parent would be asked to provide verifiable (no absolute requirement to verify) information such as last name, DOB and zip code. The PLUS could be a menu of choices for the parent including a choice to send an "I certify I am the parent" SMS message to the operator. The operator has the ability to restrict the SMS to only come from carriers that require a legal contract with an adult making the consent ultimately verifiable. The operator could then follow up with fraud detection processes that might include conducting a random sample to further verify the parent email, cell phone, name and zip against available data aggregators; or allow the parent to provide a physical address to receive a postcard in the mail which could be automated for example.

The FTC has proposed that safe harbors can aid in the approval of consent methodologies in order to provide assurance to participating members that their practices will be deemed compliant. The FTC should consider expanding that right to allow the safe harbors to approve methods that meet the level of risk along a sliding scale rather than an all or nothing approach to parent consent.

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. Researchers and the national news media have brought the obvious front and center, U13 children are using social media services regardless of the fact that most of the popular services have chosen to on the surface block U13 participation through their terms of service and age-gates. The reason that screen names and user ID's that are leveraged across multiple sites must be added to the definition of PII is in part because many of these online services have morphed into identity providers; allowing them to facilitate the delivery of U13 data to create accounts at relying party sites where 1) the relying party site is attempting to rely on the social media account as the age-gate, 2) the relying party wants to use the marketing channel to communicate to the account holder on a property other than the site they control and 3) the relying party is collecting additional personal data about the user. When these identity provider services are connected to relying party sites they have the ability to share and amass a tremendous amount data, to track the account holders' use of the relying party sites like a beacon and to offer a new marketing channel to the relying party. The fact that these social media services/identity provider services rely on actual knowledge based on an age-gate gives them a lot more wiggle room than a site that wants to allow children to legitimately participate.

Industry, Parents and Kids will lose if the distinction between directed to children, teens and general audience is not better defined. Retaining the actual knowledge standard is not worth arguing. However, sites that choose to block U13 even when there is evidence that kids are actively registering with or without parents buy in should have to do something reasonable to make sure that it is not so easy for the U13 to lie to the operator. It is ridiculous that kids whose parents would otherwise be willing to permission their child are instead forced to lie. It is equally ridiculous that a parent of a U13 child truly has no way to stop their child from fibbing at an age-gate and that operators can maintain a "head in the sand" approach to gaining the knowledge they would otherwise need to react to. If a site blocks U13, and they provide a means for delivering a portable identity then they should not accept advertising revenue or other monetary compensation when the relying party site is obviously directed to

U13. Therefore by accepting the connection the identity provider should be considered to have actual knowledge that the data they are sharing and receiving likely involves a U13 child.

The right to claim general audience or teen directed is a huge advantage because it allows for the actual knowledge standard to be the measure for whether further COPPA protections are required. The site that is directed to children loses the right to an age-gate; thereby having to assume all data collected is coming from a U13. If the sliding scale of consent is flattened they will have a huge burden to overcome to the benefit of those services that can hold out as general audience or even directed to teens. The problem is that 1000's of brands are anxious to engage the U13 demographic and they want to provide U13 with ways to interact with the brand through social media. The simple buckets of directed to children, directed to teens and directed to general audience is not workable. It has been long understood that if the service is directed to children then we must process parent consent for any collection, use and disclosure opportunities. That means we have to assume all users are U13 and obtain parent consent if necessary regardless of the child's real age. If the site is directed to teens or general audience then they can age-gate and provide a U13 parent consent path or simply turn away the U13 from registration. So what do we do with the very common example of a site that is truly overlapping between U13 and teens? For example a site directed at 9-14 year olds. It is not clear whether we can use an age-gate. If we can, and if the sliding scale is eliminated then likely all users will age up to avoid the parent consent hassle. Another likely problem with an overlapping site is how do we justify the site promoting the use of an SNS or other social media account that publicly states it does not allow U13? Can a site attracting 9-14 use the SNS account existence as an age-gate? Does our example site have the right to encourage users to "like" the site? Whereby data of the user is provided to the site owner through the fan page and a marketing channel much more robust than any marketing through an email or IM is created?

COPPA should not be seen as a ban on marketing to children U13. 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). The argument that if a user is anonymous, meaning the site does not know who the user actually is, but the anonymous users' actions are being tracked so that an operator can target marketing efforts then does it really matter that the user is anonymous. COPPA is a marketer's law first and foremost.

We agree with the FTC that new parent consent processes or innovations need not obtain specific FTC approval. 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". At this time there is no scalable and reliable method being utilized that makes even an attempt to verify that the adult providing consent is actually the parent or guardian of the child. This is a gaping hole in the current implementation of COPPA.

As an FTC approved safe harbor we speak from a unique vantage point. Not only have we consulted and certified all types organizations including commercial, government and not-for-profit 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.

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 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. Online services that are attracting U13, not parents, are creating a generation of fakers by not providing parents with reasonable methods to provide consent. Kids and parents are in a very bad position because the large sites that KNOW they have U13 kids are able to hide behind actual knowledge. This is critically important when the large sites that come to mind are the ones who are providing the marketing real estate for sites to attract fans, the stores to download apps and the email and SMS services needed to reach users.

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 to utilize their services 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.

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.

Relaxing the need for parent notice and consent to allow U13 to access social features that might allow for the disclosure of PII is problematic. Under the new proposed guidelines, 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 that eliminate "all or virtually all" PII. I am not clear on what "all or virtually all" is. 100% was never really achievable. Would nine out of 10 times the PII is deleted be considered virtually all for example? Is this the same as if a reasonable person would have identified and deleted from communication obvious PII before the disclosure is made public? Best efforts are going to be very difficult to measure. Can the FTC 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?). Operators are going to look to safe harbors to certify their compliance in this area. That means that the risk of getting it wrong is going to

potentially shift to the certifying entity. This new reasonable measures standard is based on that fact that everyone recognized that crafty kids will achieve success in circumventing systems that are attempting to allow freedom to express, but at that same time do a damn good job of keeping PII from being disclosed. If what is being acknowledged is the fact that crafty kids will get around these systems, and that we can't burden all constituents with obtaining meaningful consent to protect the few, then shouldn't we at least admit that PII will get through and that some level of exposure is reasonable given the conversion burden and cost of obtaining consent BUT that because it is reasonably possible that kids who take the effort will be able to disclose PII we should at least be required to notify the parent. Wouldn't this still be a good use of a less reliable method and potentially kids would be better served by some level of parent opt in versus none?

The combined methods used to achieve the new bar are hard to define, build, mandate and audit. The elimination of the need for parent consent should be seen as an exception to prior verifiable parental consent. The obvious ability for the disclosure to happen should at least warrant the same parent notice and opt out right that is required for collecting and retaining an email from a child for password reset (note that account administration should not be limited to password reset but should include user authentication to the site). Isn't the likelihood of circumvention at least as risky as a child signing up for a generic newsletter or contest that would otherwise require parent notice with the right to opt out?

What bundle of safety measures will truly mitigate 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 a U13's first and last name, physical address or cell phone. How about the child who discloses their SNS account or IM for example? Legal departments will want to mitigate the risk to their operators if they chose to bypass parent consent and instead find ways to truly restrict PII disclosure. The problem is that as much as companies try to use white list for acceptable communication the business and marketing teams are under a lot of pressure to add words and phrases to keep the communication real. At some point the system may not do a good job. What about the operators who can't afford to buy a sophisticated service and instead will be building their own home grown filtering using dictionary list of thousands of words? There will be a lot of responsibility and pressure on the organizations doing the compliance certification to evaluate sophisticated technology. I recommend that the safe harbor be given the right to put management of our members on the hook for the claim that "all or virtually all" PII is deleted. If management does not hire specialist services to accomplish the goal of mitigating PII disclosure then management should be required to certify its claim and should not be able to then disclaim the potential disclosure in their privacy policies and terms of service.

Other Considerations:

If a site is truly directed to children U13 then the FTC should consider the difference between a site directed for example to 5-7 and a site directed to 8-12. Currently, if a site or application is directed to children U13 then we have to assume the registration is initiated by the child. If a site for younger kids wants to communicate with a parent through email or SMS regarding their child's use of the site or to continue to market the service then how will that be accomplished? It seems over kill to have the parent in this situation have to take on parental consent at the highest level when they are likely the one providing their own PII. This would be a perfect use for the current method of email+. So, is it possible that the current implementation of email+ has a use with the younger kids whose parents are likely to be directly involved in the initial registration or application download? This would certainly reduce the potential burden that small mobile application developers are going to face. Not to mention

how reasonable it would be for toy companies who often segregate their toys by age groups that are subsets of the U13.

Clarification is needed for industry as it relates to the ability for an operator to communicate to a previously verified parent through any reasonable means that the parent selects for additional privacy and safety notices or future request for consent. For example, once a parent has established a parental relationship that is being relied upon by the site or service they should not be forced to use online contact data as their only means of receiving communication. If the parent wants to provide their mobile number and use SMS as the preferred means to receive communication from a site or application that choice should be expressly permitted. Although I believe this to already the case it needs to be clarified. Again the new contact data is being provided by the verified parent.

Currently a screen name that reveals an individual's email address is considered PII. Shouldn't this be a screen name that reveals online contact information and not be limited to an email address?

The proposed change in personal information to include IP or unique device ID should allow for the use of an analytics service if indeed its sole use is for servicing the site and it is not used to garner information about the user that the site would not have otherwise known. The problem is that once the data is fed to the analytics company it is likely merged into a larger database and by its very nature the analytics service has information that it might repurpose for its own use. This area needs more thought as it is possible that this practice may be able to fall under an exception.

The proposed amendment to Sect. 312.5(b)(2) should be revised to say "*provided that* the parent's government-issued identification is deleted by the operator from its records..." it is critical that the deletion of data relates to the sensitive data that is the government-issued identification and not to the parent's name or address for example. Also, if a parent is going to be given the option of sending in a utility bill or copy of a government issued ID then the site has the extra burden of managing sensitive and personal data that is potentially maintained in hard copy. This is a process that should not be taken up by individual companies although it may be reasonable for an infomediary service whose business it is to process identity verification to do so.

Electronic scans of a printed and signed form are as simple as 1) printing, signing and taking a picture with a smart phone to email off the image or 2) copying a signature.gif for example into the online form, saving the form as a pdf and emailing off as if it was a scanned image. For this reason scanned images should require a hand written date and parent name alongside of the signature. This will eliminate the simple cut and paste job and will aid customer service in knowing the signature is reasonably legit.

The Commission proposes to amend Sect. 312.5(c)(2) to allow for the collection of a parent's online contact information to notify a parent the child is participating in a site that otherwise does not seek to collect any personal information from the child. This exception should allow for the collection of the child's first name so that the notice can be more easily recognized by the parent. This would apply to 312.5(c)(4) as well. Additionally, the exception states that the parent information cannot be used for any other purpose. It is not clear then if the site can use the notice exception to request or offer a parent to opt-in to communication from the site directly to the parent. This has been a very common practice amongst sites that would prefer to market directly to the parent. In the past it was not a problem because the opt-in would be converted to an email plus type of opt-in and therefore, it has always been possible for a site to direct its marketing efforts to the parent once the consent was in

place, even though the initial collection of the parent information was provided by the child initiating registration. If however, email plus is going be eliminated it would mean that a site would have to get full on VPC in order to communicate any marketing to the parent. This was discussed in the example site above directed to parents and 5-7 year olds above. Please clarify this in the final review. This is potentially a huge loop hole that will cause tremendous friction if it is not clear to site operators that they need to and can obtain parent opt-in to parent communication and what steps have to be taken to verify the consent.

Sect. 312.5(c)(1) has always been puzzling in that it states "collecting a parent's online contact information and the name of the child or the parent". This should be clarified to be child's first name. Also, it has never been clear why this particular exception allows for the operator to collect the parents name from the child. I have never seen a circumstance that this would be necessary. Shouldn't parent name be eliminated, and if not please clarify if this is first and last name?

Regarding the new requirement of the safe harbor to report to the FTC "a description of any disciplinary action taken against any subject operator..." This could have a chilling effect on a company's interest in joining a safe harbor. I expect the concern of potential members and their attorneys will be that by joining a safe harbor to make a best effort to be in full compliance of COPPA, the operator is actually drawing a spotlight of scrutiny by the FTC. Please confirm that disciplinary action is related to the fact that a site has refused to do what is necessary to comply with the safe harbor guidelines and not that each time a site makes a potential mistake they are now at risk for having it reported to the FTC regardless of the fact that they are willing to correct the problem in a timely manner?

Privo appreciates the opportunity to provide these comments to assist the Commission with its continued 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
Privacy Vaults Online, Inc. d/b/a PRIVO
dtayloe@privo.com
703-932-4979