AssertID, Inc.
Belmont, CA 94002
www.assertid.com

September 18, 2012

By Electronic Delivery

Mr. Donald S. Clark
Secretary of Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, DC 20580

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

Dear Mr. Clark,

AssertID welcomes this opportunity to comment on the proposed amendments to COPPA and we appreciate and support the FTC's efforts to revise the Rule to keep pace with rapidly evolving technology. We feel strongly that this process must be continuous if COPPA is to remain relevant and to have the desired effect.

About AssertID, Inc.

AssertID is a privately held, for-profit company specializing in Identity Verification and Privacy Protection services. AssertID is currently in closed-beta of a web-based verifiable parental consent service and are finalizing our service's UX in preparation for our submittal to the FTC for review and approval upon implementation of the new COPPA Rule.

1. Verifiable Parental Consent

A. Elimination of the "email plus" parental consent method

AssertID supports the FTC's move to eliminate "email plus" as an acceptable means for obtaining verifiable parental consent. Not only do we support the assertion that email plus is insufficiently robust and easily circumvented, but we also believe its continued acceptance has in the past, and would continue in the future, to serve as a disincentive to the development of more robust and innovative alternative solutions.

It was the prospect that "email plus" would likely be eliminated that contributed significantly to AssertID's decision to respond to the FTC's call for innovative solutions

and to devote resources to the development of our parental-consent service. Through this service AssertID addresses what we believe to be the two greatest impediments to COPPA compliance:

1. The high-cost and operational complexity for an operator to request and receive verifiable parental consent and;

2. The intrusive and cumbersome processes by which parents can currently provide such consent.

B. Commission and Safe Harbor Approval of Parental Consent Mechanisms

Although AssertID supports the broadening of the list of acceptable methods for obtaining verifiable parental consent, we are not convinced that the newly added methods (i.e. video-conference and verification of government issued identification), offer significant relief from the shortcomings that have impeded the adoption of the currently approved methods. Like their predecessors, we believe these new methods to be too cumbersome or intrusive for parents to use and too process intensive and costly for operators to implement and are therefore unlikely to gain wide acceptance

AssertID supports, and has made significant investments in response to, the proposed revisions to 312.5(b) (i.e. the addition of paragraphs 3 & 4) which would provide for the submittal of new solutions for consideration, and would allow for Safe Harbors to approve parental consent methods not currently enumerated in paragraph 312.5 (b)(2). The Safe Harbor Approval allowance will offer operators the benefits of having access to new parental consent methods while the developers of such methods (like AssertID) are in the process of obtaining formal FTC approval.

To further speed the introduction of new parental consent methods we request that the FTC consider shortening the approval process from 180 days to 90 days.

2. Direct Notice to Parents

AssertID fully supports the FTC's assertion that the "direct notification" to parents represents the best opportunity to inform parents of the operator's information practices. We believe that this "direct notification" takes on even greater significance with mobile applications and games, where the child's initial request for access to a game or application will often be through a third-party app-store (e.g. iTunes or Google Play) and where the "online notification" on the operator's (or application developer's) website might not be readily available.

Mobile devices and third-party app-stores will often represent a "parent not present" use-case, where information usage policies presented on the mobile-app splash screen may never be seen by the parent. Also, in such cases, the "direct notification" to the parent may tie parental-consent to the application purchase authorization.

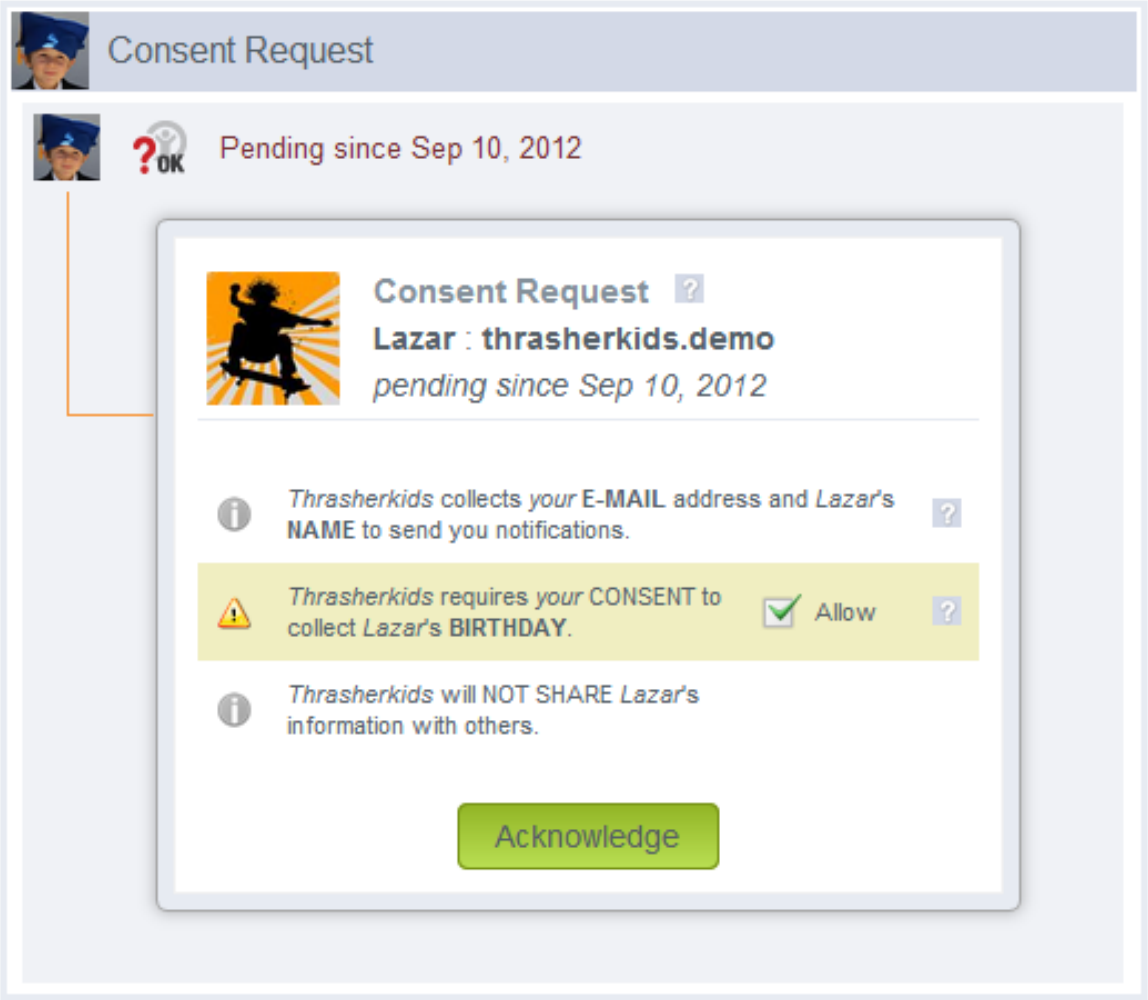
Furthermore, we are comfortable with, and support the specific language segment of, the proposed revision to paragraph (c) of 312.4:

"An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of the child's personal information, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented."

We feel this language is clear and yet appropriately non-restrictive regarding the means of presentment of these "direct notices". This is of particular importance to AssertID as our service will offer what we will promote as a standardized and easily understood format for presentment of these parental direct notifications.

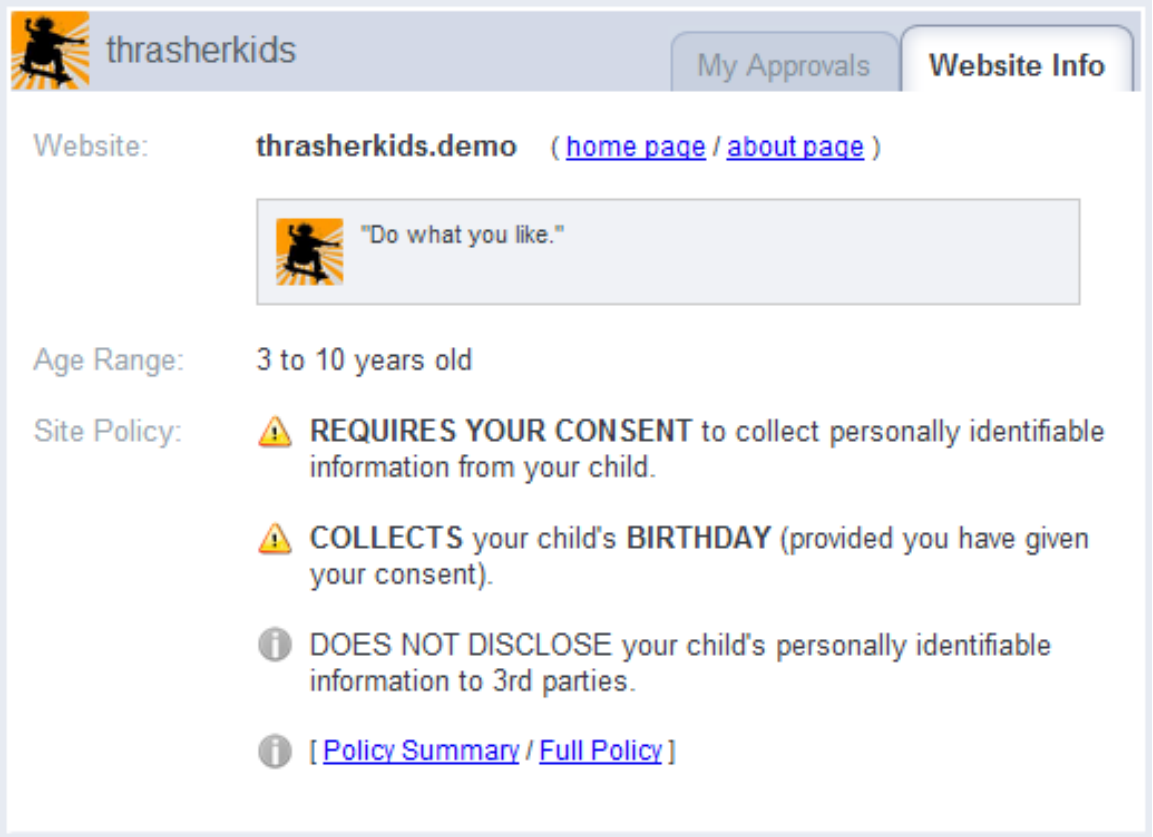
Our belief is that in so doing we will serve the needs of both parents and operators. Parents will have access to all relevant information necessary to make an informed decision, presented in a consistent, easily understood format, and operators will be able to provide all relevant information necessary to formulate such notifications through an online "fill in the form" process obviating the need for each operator to design and develop custom presentment methods.

Our presentment process will provide some of this information to the parent in association with the specific request. And the design of our browser-based solution allows a parent to grant consent from their mobile device. We will offer a native mobile application for iOS and Android devices in the future.



Note: presentment design is still being refined and will likely change before the general release of our service.

The remainder of this information is available on-demand at any time a parent might wish to review it.



Note: presentment design is still being refined and will likely change before the general release of our service.

3. Definition of "Operator" and its implications for "App-stores"

We request clarification of where services such as iTunes, Google Play and other similar "App-store" services fall within the scope of COPPA. By our reading, they do not fall within the proposed definition of "Operator" however, because they serve as the distribution point for games and applications directed at children, they might reasonably be interpreted to be a Web site or service directed at children. This position might present significant COPPA compliance challenges regarding "online notifications" and parental consent.

4. Adding Geolocation data to the definition of PII

We support the broadening of the definition of PII to include geolocation information. We are not convinced by the argument made by some that such geolocation data applies to a device and not an individual. We believe that with the continued growth of the smart-phone and mobile-device markets and the resulting lower price-points for such devices, the shared-use of mobile devices will decline, resulting in a one-to-one association between a device and an individual. This will make it increasingly easy to combine geolocation data with other information to identify a unique individual and could significantly broaden the meaning and implications of behavioral marketing.

Thank you for this opportunity to comment on this important issue. AssertID is committed to the task of providing innovative solutions to the Parental Consent Mechanism and we look forward to working through the FTC approval process in the near future.

Sincerely,

Keith Dennis
President, AssertID, Inc.