

AssertID, Inc.
Burlingame, CA 94010
www.assertid.com

September 29, 2014

By Electronic Delivery

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

Re: AgeCheq Application for Parental Consent Method, Project No. P-145410

Dear Mr. Clark,

AssertID welcomes this opportunity to comment on the AgeCheq application for approval of a new verifiable parental consent method under the COPPA Rule. As per the instructions in the request for comment notification, we will address the specific questions posed by the FTC individually. In addition we offer for your consideration comments on other “non-compliance” concerns with the proposed AgeCheq RCCM system that transcend these questions.

In response to question #1:

We can find no indication of a new parental verification method in the AgeCheq application. The only verification methods mentioned in the application are existing FTC approved methods as specified in section 312.5(b)(1) of the Rule. In our opinion AgeCheq is not requesting approval of a verification method rather; they are requesting that the FTC approve a common consent management system that uses currently approved methods. AgeCheq in fact makes clear this distinction in their description of their “Real-Time Common Consent Mechanism” provided below (emphasis added):

“This real-time, device-based, common consent management system (“Real-Time Common Consent Mechanism,” or “RCCM”) allows parents to complete a single, COPPA-compliant verification process, which may then be overlaid across apps produced by participating developers. The RCCM materially extends currently enumerated verification methods (credit card, faxed/emailed form, for example) by adding real-time, hubbed parental identification, notice, and consent management for multiple apps and devices (desktop, tablet, and smartphone), as depicted in Figure 2, below.”¹

Although we acknowledge that there are significant benefits to be gained from a well designed multi-tenant consent management system, (AssertID offers such a system), these systems do not qualify as parental verification “methods”.

Therefore, because the AgeCheq application is not for a new parental verification method as defined under COPPA, we don't believe it meets the criteria for consideration under Section 212.12 (a) of the Rule.

However, because the FTC specifically asked for comments on the “...process for obtaining consent for an initial operator and any subsequent operators...” we feel compelled to comment on what we believe are inherent deficiencies evident in the “process” as represented in AgeCheq's “RCCM” system.

All comments offered here are based upon the information provided in the AgeCheq application.

AgeCheq's RCCM seems to be based on the underlying assumption that a mobile device-ID is a reasonable proxy for a child; furthermore, that a device (not a child) is an acceptable basis upon which to request parental consent and that should a parent grant consent to such a request, that this consent is specific to a child.

We feel that this assumption is fundamentally flawed in part because it presumes:

1. that only a single child will have access to a device and thereby access to the applications on an approved device,
2. that the parent would know which child a request originated with, absent this information being contained in a request or a child ever be challenged to provide their parent's online contact information,
3. that parents would never wish to selectively approve an App. for use by one of their children and not for other children sharing the same device,
4. that a parent could know with any certainty, that a consent-request actually originated with one of their own children. Because a parent is responding to a request from a device (not a child) the request could originate with any child having access to the device, including pre-teens who are not their children.

Additionally, under the AgeCheq RCCM service an operator is never required to challenge a child to provide a parent's “online contact information”. The ability of a child (not a parent) to provide this information at the time a new application is accessed represented a link (however tenuous) between the child and parent which is totally absent from the RCCM process.

We do not believe that the use of the device-ID as a proxy for an individual or individuals is a viable system for providing parents with verifiable and granular control over the collection and use of PII from their children. We believe this loose association of a device with a child is fundamentally flawed and introduces potential exposures to children's personal information.

Using the RCCM system, an App. (operator) is not requesting permission for a specific child to use an App., rather they are requesting permission for the App. to be used by whoever has access to the mobile device.

In response to question #2:

We do not consider AgeCheq's application to represent a new parental verification "method" and therefore we do not believe it qualifies for consideration under Section 312.12(a) of the Rule.

In response to question #3:

We believe that the AgeCheq RCCM system presents significant risks to the unauthorized collection and sharing of personal information.

As described in the AgeCheq application, the RCCM system does not obtain parental consent for a specific child to use an App., but rather it obtains consent for an App. to be used on a specific device. There is no mechanism in evidence to prevent a pre-teen (perhaps a friend of the owner of the device) from accessing an App. (approved for the device) and potentially creating their own App. account through which they can share personally identifiable information.

There is no evidence that the RCCM system can provide any assurance that a specific device will not be used by multiple children (from the same family) to access Apps. Therefore, a parent could unintentionally grant consent for one or more children to access an App. mistakenly believing the request originated with a different child. This limitation does not provide a parent with selective, granular control over which of their children should have access to specific Apps. and therefore could result in the unintended disclosure of a child's PII.

Possible COPPA non-compliance Issues

Although the following issues do not fall within any of the specific questions posed in the FTC's request for public comment, we feel these potential non-compliance issues are significant enough to warrant comment.

Non-compliance issue #1

Based upon AgeCheq's description of the RCCM system process flow, it appears that for an operator to use this RCCM system, the App. (operator) must collect the device-ID before they have obtained parental consent.

The device-ID is "personal information" as defined under the COPPA Rule. Because this device-ID does not fit the definition of "online contact information" but is used to contact a specific individual (presumably the child's parent) it does not qualify as "support for internal operations" as defined under COPPA. Therefore, in order for an operator to use the AgeCheq RCCM system they would be in violation of the COPPA Rule for having collected "personal information" (the device-ID) before having obtained consent.

Non-compliance issue #2

AgeCheq's application makes the following claim (emphasis added):

"This real-time, device-based, common consent management system ("Real-Time Common Consent Mechanism," or "RCCM") allows parents to complete a single, COPPA-compliant verification process, which may then be overlaid across apps produced by participating developers. The RCCM materially extends currently

enumerated verification methods (credit card, faxed/mailed form, for example) by adding real-time, hubbed parental identification, notice, and consent management for multiple apps and devices (desktop, tablet, and smartphone), as depicted in Figure 2, below.”²

Assuming this is an accurate representation of AgeCheq’s RCCM system, a user of such a system would be in violation of the COPPA Rule should a “single” credit card transaction be accepted as verification for multiple Apps. The COPPA Rule clearly states that each individual consent relying on credit card verification must be associated with a separate monetary transaction.

Summary

In summary, we request that the FTC deny AgeCheq’s application for the following reasons:

1. Their application does not qualify for consideration under Section 212.12(a) as their application is not for a new parental verification method. The only verification methods referenced in the application are those already covered under section 312.5(b)(1),
2. AgeCheq’s RCCM system fails to satisfy the requirement for parental consent as specified in 16 CFR 312.5(b)(1),
3. AgeCheq’s RCCM system poses significant risks for the “unauthorized” collection, usage and sharing of personal information,
4. It is questionable whether an Operator using the AgeCheq RCCM system would be in compliance with COPPA because in order to use the system an Operator must collect PII (the device-ID) before they have obtained parental consent, and
5. A user of the AgeCheq RCCM system would be in violation of the COPPA Rule if they were to accept a single credit or debit card transaction as verification for multiple application approvals.

References:

^{1, 2} - Presumably pg. 28 (page is not numbered). Last paragraph on page immediately preceding page labeled 29.

Sincerely,

Keith Dennis
CEO, AssertID, Inc.