

Tom Strange, jest8
c/o Davis & Gilbert LLP,
1740 Broadway,
New York, NY, 10019

September 29, 2014

Division of Privacy and Identity Protection,
Federal Trade Commission,
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

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

This document responds to the FTC request for public comment. It addresses the specific questions put by the FTC in addition to further observations about implementation of the methodology by its sole operator AgeCheq where relevant.

It is acknowledged that the Commission approves the method of verifiable parental consent submitted for consideration, as opposed to the operator proposing to implement such method. However, in view of AgeCheq being the sole provider of the proposed method and likely intellectual property protections taken to prevent other operators implementing the method, this submission makes reference specifically to AgeCheq to assess the method against the requirements of COPPA.

Executive Summary

1. Is this method, both with respect to the process for obtaining consent for an initial operator and any subsequent operators, already covered by existing methods enumerated in § 312.5(b)(1) of the Rule?

The proposed method is *not already covered* by existing methods enumerated in § 312.5(b)(1) of the Rule.

The proposed method enables the provision of consent only when five distinct processes have been completed.

- i. An account is created with a common consent administrator (CCA) and provider of a “device-based, common consent management system” – referred to as the Real-Time Common Consent Mechanism (RCCM)
- ii. An identity must be verified against the RCCM account

- iii. A device is attached to the RCCM using the device persistent identifier
- iv. Consent requests pertaining to a device are managed by the RCCM operator
- v. Developers embed code within their apps to obtain consent from the CCA

No such method is enumerated under the COPPA rule.

2. If this is a new method, provide comments on whether the proposed parental consent method, both with respect to an initial operator and any subsequent operators, meets the requirements for parental consent laid out in 16 CFR 312.5(b)(1). Specifically, the Commission is looking for comments on whether the proposed parental consent method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

The proposed parental consent method *does not meet the requirements* for parental consent laid out in 16 CFR 312.5(b)(1). The method *is not reasonably calculated*, in light of available technology, to ensure that the person providing consent is the child's parent; to the extent that it poses a threat to children. The method fails on all five distinct processes that together form the method.

3. Does the proposed method pose a risk to consumers' personal information? If so, is that risk outweighed by the benefit to consumers and businesses of using this method?

Yes, the proposed *method poses a risk to consumers' personal information*. The risk to consumers' personal information benefits businesses and more specifically AgeCheq, to the detriment of consumers. The risk is *not outweighed by the benefits* of using this method and AgeCheq being approved to provide it.

Conclusion:

The method does not meet the requirements of 16 CFR 312.5(b)(1) and poses a risk to consumers' personal information. The manner in which the method is presented creates a false sense of assurance to all parties and would appear to create more harm than benefit. Existing enumerated methods and other general parental consent platforms that are known to the market provide a higher assurance level.

AgeCheq is the sole operator of the method and appears to engage in practices that conflict with the FTC, such as bait and switch techniques, misrepresentations and omissions. Approval of the method would be counter to the FTC Strategic Goal to protect consumers and its Mission to prevent business practices that are unfair to consumers. The threat this service poses is detailed in this submission.

The submission also finds that approval of this method could lead to social exclusion that would disadvantage underprivileged children.

Detail in support of the conclusion that *the method should not be approved*

1. Is this method, both with respect to the process for obtaining consent for an initial operator and any subsequent operators, already covered by existing methods enumerated in § 312.5(b)(1) of the Rule?

The proposed method enables the provision of consent only when five distinct processes have been completed.

- i. An account is created with a common consent administrator (CCA) and provider of a “device-based, common consent management system” – referred to as the Real-Time Common Consent Mechanism (RCCM)
- ii. An identity must be verified against the RCCM account
- iii. A device is attached to the RCCM using a persistent identifier
- iv. Consent requests pertaining to a device are managed by the RCCM operator
- v. Developers embed code within their apps to obtain consent from the CCA

The primary differentiator between the proposed method and other enumerated methods or general consent platforms is the use of a persistent identifier as a proxy for a child’s unique identity; linking that persistent identifier / device to a control account from which consent is issued to the specified device (not child). The method is not a combination of enumerated methods in a manner that would require no approval. The method is new and requires Commission approval against the requirements of 16 C.F.R. § 312.5(b).

2. If this is a new method, provide comments on whether the proposed parental consent method, both with respect to an initial operator and any subsequent operators, meets the requirements for parental consent laid out in 16 CFR 312.5(b)(1). Specifically, the Commission is looking for comments on whether the proposed parental consent method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent.

- i. An account is created with a common consent administrator (CCA) and provider of a “device-based, common consent management system” – referred to as the Real-Time Common Consent Mechanism (RCCM)

The method contains no process to prevent or reduce the risk of account

creation by a child under the age of 13. There is no identity verification component in the registration process and is no age screen implementation.

The design of the method is such that a child could create an account with the CAA. Although an identity verification process is subsequently completed, access to the parent area of the CAA – operated exclusively by AgeCheq – creates access to information and tutorials about the service. A child being able to obtain this information increases the likelihood that the method would be circumvented for reasons outlined later in this submission.

The operator of the CCA – AgeCheq – would be considered a general audience website or online service so it could, under the COPPA rule, block children from participating should it choose to. In light of the intended purpose of the CCA it should reasonably be expected to do so.

As a minimum the method should feature the implementation of an age screen, designed in a manner that does not encourage children to falsify their age to gain access to the CAA as a “parent”. One could reasonably argue that identity verification should be designed into the registration process flow such that no child can access the CAA. The method and its sole operator AgeCheq appear deficient in the implementation of this basic consideration.

(ii) Identity verification & (iii) where a device is attached to the RCCM, are interrelated because both are required for the proposed method to become a mechanism for the provision of consent by the operator of the CCA/RCCM

The submission asserts that step (ii) – where the RCCM controller must verify their identity – can be completed “through any currently enumerated method”. It assumes that the completion of identity verification of the CCA/RCCM account after its creation is sufficient to meet the requirements laid out in 16 CFR 312.5(b)(1) and to ensure that the person providing consent is the child’s parent. *This assumption around identity verification adequacy has been disproved.*

The Commission enumerated methods under COPPA for the purpose of providing verifiable parental consent, where a parent of the child receives notice of an operator's information practices and consents to those practices.

Under the proposed method, the point at which a parent receives notice of their child’s participation in an online service and notice of that operator’s information practices, is only after and if, the device being used by the child is linked to the CCA/RCCM account controlled by the parent. There are two processes (account

creation and the linking of all devices) where identity verification is required but the method is implemented with only one attempt to verify identity.

The method as proposed, creates false assurance because it suggests use of a “currently enumerated method”. The enumerated methods as implemented by the applicant are applied out of the context for which they were intended and originally enumerated. This misuse creates the appearance of compliance but creates an unintended threat to children as outlined herein.

ii. An identity must be verified against the RCCM account

Use of enumerated methods in a manner not intended:

The provision of consent under the proposed method (linking a device to an RCCM and sending permissions to that device) is divorced from the process of verifying an identity against the RCCM, which itself is divorced from the process of verifying the identity of the individual first registering with the CCA. The approach taken creates a higher level of threat (see section for 2iii), such that the identification of a parent becomes more critical, sensitive and subject to risk.

The sole operator of the method (AgeCheq) offers identity verification of the RCCM controller by “print-and-send” and a payment system. In order to test that the method proposed and implemented by AgeCheq meets the requirements for parental consent laid out in 16 CFR 312.5(b)(1) and is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent, the implementation of the monetary transaction method by AgeCheq was tested. “Print-and-send” has not been tested for this submission.

Framework for testing of AgeCheq implementation of identity verification:

There are general risks around a monetary transaction as a means of personal identification such as that completed with a credit card:

- Identify fraud – a card is successfully applied for in a fictitious name
- Identity theft – a card is applied for in someone else’s name

Even with valid credit card applications, identity checks prior to the issuance of a card vary considerably around the world. The United States have a higher security threshold than other global jurisdictions because credit reference bureaus have access to public social security records – even with the higher level of assurance there is a level of fraud and misuse of cards. Standards of verification in applications outside the U.S. are typically weaker.

Online security checks applied to card payments aim to verify that the holder of the card at the time of use is the authorized account holder. To process the transaction, data taken from the card is entered into a digital form. Additional security measures such as a user password can be implemented at merchant discretion. In any event a 'false' or fraudulent identity will pass these tests because the perpetrator is the holder of the card and has the information to correctly pass these verification steps, even if applied.

Results of AgeCheq testing against the framework

AgeCheq appears to use the lowest threshold for payment security because it processed a payment using an incorrect date of birth and fictitious address. No password was required. The manner in which AgeCheq identifies the RCCM controller with a monetary transaction is defective and inadequate as a means of ensuring that the person consenting (the RCCM controller) is the child's parent.

The reason this is particularly important and mitigation of fraud/criminal activity risk so crucial, is because of an inherent failing in the method more broadly set out in (iii). As implemented by AgeCheq the identity verification method does not appear to be fit for purpose. Such is the inadequacy in the method and verification process that it could perpetuate threats to child safety (see 2iii).

- iii. A device is attached to the RCCM using a persistent identifier

Risk of registering a device to an alternative administrator account (RCCM):

Under the proposed method, when a child attempts to use an app that offers AgeCheq authentication on a device that is not linked to an RCCM, the child enters the AgeCheq username of the RCCM to which they want to connect.

The attachment of the device to the RCCM is the action that leads to consent later being granted to apps on that device but there is no control or verification or mechanism to ensure that the RCCM user name provided is that of a child's parent. The method is inherently defective and does not reasonably ensure that the person providing consent (via the RCCM to which the child choose to link into) is the child's parent.

Approval of this method could pose a significant risk and threat to children. There are numerous websites set up for the posting anonymously online such as ask.fm, spring.me and apps such as Whisper in addition to anonymous forums such as 4chan.org. It has also long been the case that children use the Internet to find shortcuts and cheat codes to games they play with services such as cheatcc.com and gamesradar.com. In view of precedent child behavior and the

trend toward increasing anonymity online, it is possible that third parties (that are not the child's parent) will make AgeCheq usernames publicly available, offering to grant app approvals and or provide usernames where the AgeCheq "authorize everything" feature – a feature which in itself creates risk and is critiqued later in this submission – has already been activated. The deficiencies highlighted in the AgeCheq identity verification process exacerbate this risk.

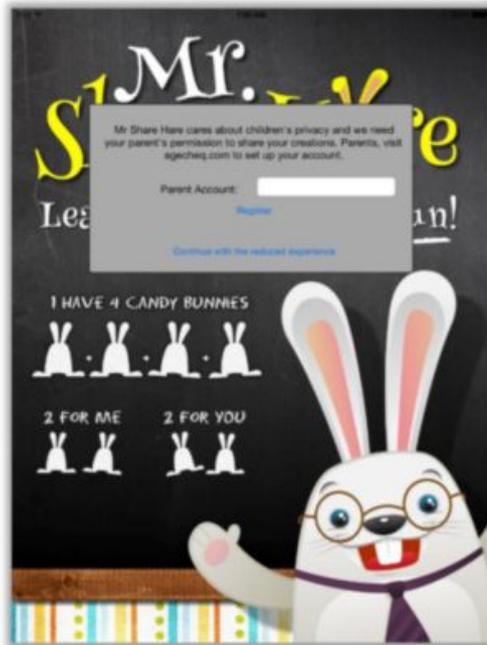
This would result in circumvention of COPPA and could create opportunities for sexual predators to use the method to groom minors by offering usernames to build rapport with children and or instigate the exchange of CCA usernames for photos of the child in question. An FBI report states, "more than half a million pedophiles are online every day" and that the "trend among pedophiles is to begin grooming youngsters through online gaming forums". Statistics from the U.S. department of justice stated, "1 in 25 youths received an online sexual solicitation in which the solicitor tried to make offline contact". The alluring and compelling incentive to children of accessing content, via the method for which approval is sought as implemented by AgeCheq, without parents knowing or needing permission, is potentially a new enabler to these predatory behaviors.

There is no evident process in the method that would prevent a child from downloading the RCCM enrollment app that the applicant refers to in Figure 3 and Figure 4 of its submission, thereby circumventing the process as outlined above. It would be unreasonable to assume that a child has no access to the password required to download apps from the relevant apps store. Parents are unlikely to know that sharing the app store password would create this risk.

As such, the proposed method could lead to children unwittingly placing themselves in harm in what evidence suggests is a very real, possible high risk scenario. The defective and weak implementation of identity verification by AgeCheq indicates that the risk is not mitigated to a reasonable level. It is apparent that criminals seeking access to children, such as sexual predators, could register with AgeCheq using identities other than their own.

The relevant process flow from the AgeCheq user support materials is included to assist in the presentation of this point. The wording assumes a parent is completing the process with no mechanism to prevent a child acting on this.

3.1 Linking Games and Apps



Enter the username you chose to sign into the Parent Dashboard when prompted by an AgeCheq-enabled game or app. The username is how you are identified on the AgeCheq system.

iv. Consent requests pertaining to a device are managed by the RCCM operator

COPPA rule explicitly states the necessity for a parent to control and manage the privacy of a *child* – to approve, decline and or revoke permissions around the collection of data of each individual *child* i.e. not one blanket system for all children within a family and not the data as it pertains to a specific device. The inclusion of the relevant legislation extract is included for the benefit of parties other than the Commission, to draw emphasis to the necessity that any method approved must enable parents manage the privacy of each individual child.

SEC. 1302. DEFINITIONS.

(9) VERIFIABLE PARENTAL CONSENT.—The term "verifiable parental consent" means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a *child* receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that *child*.

SEC. 1303. REGULATION OF UNFAIR AND DECEPTIVE ACTS AND PRACTICES IN CONNECTION WITH THE COLLECTION AND USE OF PERSONAL INFORMATION FROM AND ABOUT CHILDREN ON THE INTERNET.

(b) REGULATIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate under section 553 of title 5, United States Code, regulations that— ...

(ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;

(B) require the operator to provide, upon request of a parent under this subparagraph whose *child* has provided personal information to that website or online service, upon proper identification of that parent, to such parent—

(i) a description of the specific types of personal information collected from the *child* by that operator;

(ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that *child*; and

(iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that *child*;

(D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

(3) TERMINATION OF SERVICE.—The regulations shall permit the operator of a website or an online service to terminate service provided to a *child* whose parent has refused, under the regulations prescribed under paragraph (1)(B)(ii), to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that *child*.

Persistent identifier as a proxy for child identity:

The method put forward proposes, “linking a verified parental identity to a *specific device associated with a child*, and permitting the parent to curate the child's access to unlimited numbers of apps via a common mechanism, on a real-time, automated basis. 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 method uses a persistent identifier as a proxy for a child’s unique identity. The hurdle then, in determining whether or not the proposed method meets the requirements of COPPA, is to ascertain whether or not a persistent identifier is suitable as a proxy for a child’s unique identity; to the extent that operators can satisfactorily discharge their responsibilities under the rule and parents are able to manage the privacy of their children.

Objective Statistical Evidence:

The Common Sense Media report entitled “Zero to Eight: Children’s media use in America 2013” states that “*just 7% of children have their own tablet*”. CIA data indicates a 2014 Total Fertility Rate (TFR) of 2.01 children per U.S. Household.

A TFR of 2.01 taken with the reported statistic that just 7% of children have their own tablet, indicates a high probability that the *devices children use to engage with operators of online services are shared by at least two children in a household i.e. 93% of children to do not have a device specific to them*.

Inference from the evidence:

Evidence indicates that it would not be possible for a parent to manage the privacy and exposure of each of their children as is required by COPPA because there can only be one persistent identifier to the device.

It would not be possible for an operator to know which child's data it had collected from use of the device because there would be in 93% of instances, 2 or more children using it. It would not be possible for operators to manage the privacy of each child, for parents to request deletion of data pertaining to a child and revoke the relevant consents because multiple children (siblings or friends) could have participated on the device that was queried against the CAA database and approved for data collection as per the method.

In conclusion, it is clear that in 93% of instances there is not a "*specific device associated with a child*". A device and its persistent identifier would not pertain to an individual child and is not a suitable proxy to a child's identity. There is a statistically high probability that the method would be ineffective; that operators cannot satisfactorily discharge their responsibilities under the rule and parents would be able to manage the privacy of their children; it should not be approved.

Multiple accounts created within an app:

The method proposes that participating developers embed code within their apps that would automatically query the CCA's database to ensure parental consent has been granted for the app to allow use and collect child data.

In the absence of information to the contrary, it is reasonable to assume that an app, for example Facebook, Twitter, Pinterest, Instagram et al would allow for the creation of a user account unique to each user on any given device.

On a family shared device, as is the case for 93% of U.S. children, use of the method for which approval is sought would lead to a statistically high probability that multiple accounts would be created within one app by multiple children.

This method denies parents the opportunity to determine the appropriateness of a product or service for each of their children based on factors such as age and maturity because a query against the CCA indicating that consent has been granted, say for an older sibling, would open use of the app to younger sibling.

In his submission Mr. Smith claims "the RCCM could even promote the creation of innovative new apps for young children" and "requests that the Commission

act favorably” to his application on that basis. It is widely reported that entities such as Facebook and Google would like to provide products and services to the under 13 demographic. It is reasonable then to conclude that the innovation Mr. Smith refers to could well include the provision of apps that facilitate the disclosure and sharing of personally identifiable information by children in a public and social domain, such as Google+ and or Facebook.

This submission passes no comment on the suitability of these products and services for children but does suggest that a method that denies parents the opportunity to control the use of such services by each of their children, fails to meet the requirements of COPPA and should not be approved.

In the event that AgeCheq provided further information to that made available for public comment, asserting that only one account could be created per app/per device persistent identifier, this would result in multiple children using one account. The end result would still be the disclosure and dissemination of personally identifiable information, potentially in the public domain, pertaining to multiple children for which consent has not been given.

If all AgeCheq compatible apps were required to permit only one-sign per device persistent identifier, as checked against the CAA database, this would be onerous to the industry and developer community and inconsistent with either current industry practices or the direction of travel.

Devices used within friendship groups:

As documented under the heading “Multiple accounts created within an app”, the method proposes that participating developers embed code within their apps that would automatically query the CCA 's database to ensure parental consent has been granted for the app to collect child data.

The same mechanism that would allow multiple siblings to create a profile would enable friends to create an account on the device to which consent was granted by the parent of another child.

It is unclear whether or not an account created with an app such as Google+, or Facebook (if those operators integrated the AgeCheq SDK) would also be accessible from other devices or through websites not linked to a CCA or device on which they were initially created. Such operability could lead to numerous instances of children using products and services where the person providing consent is not the child’s parent, but was a friend’s parent. The friend’s parent would also be unaware that they facilitated the breach of Federal regulation. The

parent of a child that created the user account on a friend’s device would also have no reasonable means of knowing that their child had done so.

The proposed method could exacerbate the risk of non-compliance with COPPA and in light of available technology *does not provide adequate safeguards to ensure that the person providing consent is the child’s parent.*

Mechanism enabling no parental consent process – “authorize everything”:

AgeCheq provides parents with an “authorize everything” button for “adult accounts”. Both the proposed method and AgeCheq service are positioned as a product to facilitate COPPA compliance. COPPA applies only to children under 13 so adults have no clear reason to register with apps using AgeCheq.



(Username and email have been removed for protection of privacy)

There is no clear rationale for the inclusion the “approve everything” functionality. It appears to perpetuate non-compliance with COPPA by enabling one to forgo providing consent. It is confusing to parents because the service is put forward as method of protecting the privacy of their children – not for adults.

It is unclear why AgeCheq asks for birth month and year of each child yet also includes this functionality because its system could detect whether or not this was relevant. If “authorize everything” was selected and AgeCheq had recorded the details of a child under 13 in one of the profiles, AgeCheq would be in breach of COPPA; knowingly enabling the collection of PII from children under 13 by third parties without parental consent. *That scenario was tested and is possible.*

In the absence of further information it would appear that this further supports that position that this method does not meet the necessary requirements.

v. Developers embed code within their apps to obtain consent from the CCA

In the documents submitted for public comment it states, “developers are responsible for incorporating the RCCM into their app and ensuring that approval

or rejection responses received from the RCCM are responded to appropriately (by unlocking the app or leaving it blocked)". This suggests scope for circumvention within the method proposed however the applicant has provided insufficient supporting information to adequately assess this risk.

3. Does the proposed method pose a risk to consumers' personal information? If so, is that risk outweighed by the benefit to consumers and businesses of using this method?

Yes, the proposed method *poses a risk to consumers' personal information*. The risk to consumers' personal information benefits operators and more specifically AgeCheq to the detriment of consumers. The risk is not outweighed by the benefits of using this method and AgeCheq being approved to provide it.

Review of AgeCheq as a methodology and operator has revealed material representations, omissions, and practices that when considered from the perspective of a reasonable consumer, are likely to mislead parents.

Specifically, there appears to be use of bait and switch techniques in conjunction with misleading price claims, false oral and written representations and a product that is systematically defective without adequate disclosures.

As defined by the Commission these misrepresentations, omissions, and practices are presumptively material because they fall in the category of express claims - where the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false.

Evidence also appears to exist that the AgCheq intended to make implied claims likely to mislead consumers. The Commission has previously stated it would infer such implied claims as material so they too have been included herein.

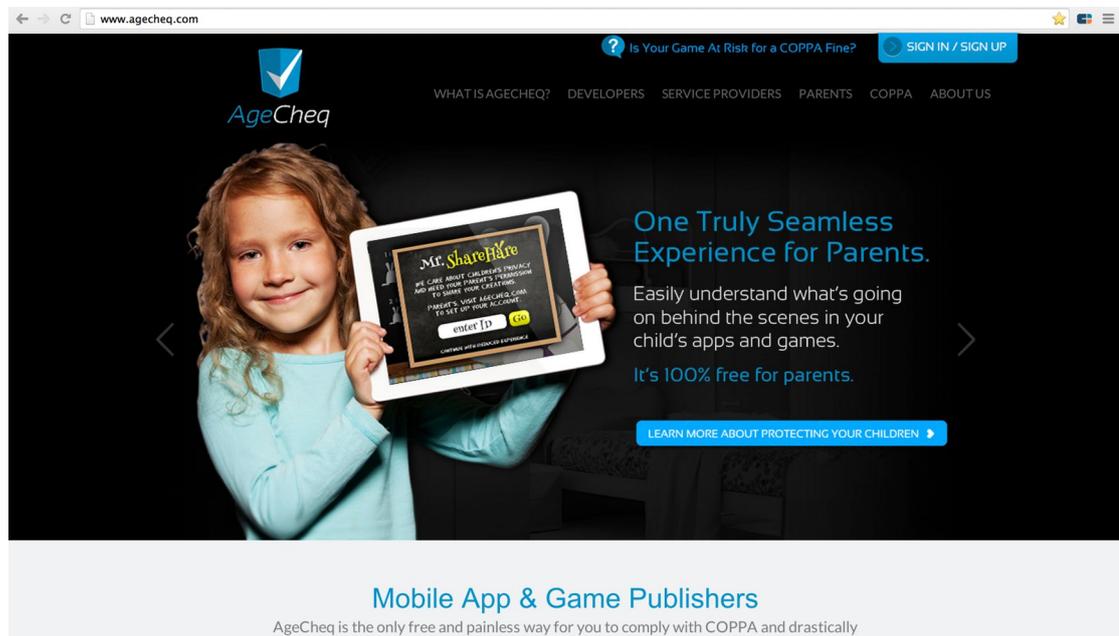
Furthermore the Commission considers claims or omissions material if they significantly involve health, safety, or other areas with which the reasonable consumer would be concerned.

In view of this product being related to the provision of child privacy it is considered as an area with which the reasonable consumer would be concerned and a full disclosure of findings has been made.

A product that is systematically defective without adequate disclosures

Disconcerting privacy policy implementation

AgeCheq asserts, “by approving this method, the Commission can enable developers to comply with the COPPA rule and empower parents to make informed decisions about their children's online privacy”. The website and all user process flows in registration reinforce that AgeCheq is a product that supports and enhances privacy.



A review of the AgeCheq privacy policy indicates that the product is systematically defective without adequate disclosures. Ironically AgeCheq suggests that it enables more informed decisions to be made about child's privacy but designed its own privacy process so that parents do not make informed decisions. It would appear that AgeCheq is designed as a marketing and analytics platform but is not transparent to its users – parents and children..

http://www.agecheq.com/?page_id=217

Privacy Policy Extract:

Sale of data:

“We may share aggregated and anonymized information with any third party”.

Assumed acceptance of the privacy policy:

“By using the AgeCheq Service you acknowledge and consent to such use” [of your data].

During the registration process there is no requirement for a parent to accept or read the privacy policy of the company. There is also no reference within the user experience that explains to parents that their data is used for marketing purposes. In light of the fact that the proposed method and AgeCheq put themselves forward as furthering consumer privacy, this clear and apparent choice not to conform even to industry best practice is disconcerting.

AgeCheq could for example have adopted explicit consent by including following check box as implemented by Google:



Implicit consent taken on policy revisions:

“AgeCheq reserves the right to modify this policy at any time. Any such modifications will be effective as and when posted on the AgeCheq Service. You are responsible for reading and understanding the terms of this privacy policy prior to using the AgeCheq Service. Your use of the AgeCheq Service after any such modification has been posted constitutes your acceptance of such modifications to this privacy policy.”

In the first instance AgeCheq obtains no consent. It then maintains the right to make changes without notification or further acceptance. This poses a threat to parent data and also to child data, which could subsequently be made available. It is unlikely, in view of privacy policy acceptance being implicit that parents would be aware of the threat that AgeCheq poses to them and their children.

Marketing and analytics based revenue models

Let me be clear on my position. Revenue models based on marketing, analytics and or advertising, are widely known of and accepted by consumers in society. Such a revenue model enables consumers around the world to enjoy digital products and services that they would otherwise have to pay for directly. Review of websites visited by U.S. citizens’ supports that assertion and general consumer receptiveness to a business model where revenues are generated in this way.

<https://www.quantcast.com/top-sites>

RANK	SITE	MONTHLY PEOPLE
1	 google.com	203, 733, 280
2	 youtube.com	187, 089, 760
3	 facebook.com	138, 880, 752
4	 msn.com	115, 775, 824
5	 ebay.com	105, 027, 632
6	 Hidden profile	—
7	 yahoo.com	92, 498, 048
8	 twitter.com	88, 847, 592
9	 amazon.com	80, 680, 880
10	 yelp.com	74, 458, 320

In this instance however it is deceptive of AgeCheq not to make it clearer to parents what AgeCheq truly is and does. It is deceptive not to require explicit acceptance of the privacy policy where this is detailed. It is unacceptable that AgeCheq retains the ability to revise its privacy policy to include dissemination of parent PII or child PII at anytime without requiring explicit consent from parents. There is a clear absence of transparency yet, as a recently formed company, AgeCheq had an opportunity to proactively manage its relationship with parents and make its intentions clear at the outset.

The behavior of AgeCheq is at odds with the FTC Mission and Strategic goals and indicates that AgeCheq is not suitable as an enabler to the processing of parent-child data under the proposed method, or in fact any other. Both the method and its sole operator, AgeCheq, pose a risk to consumers' personal information that is no outweighed by the benefits.

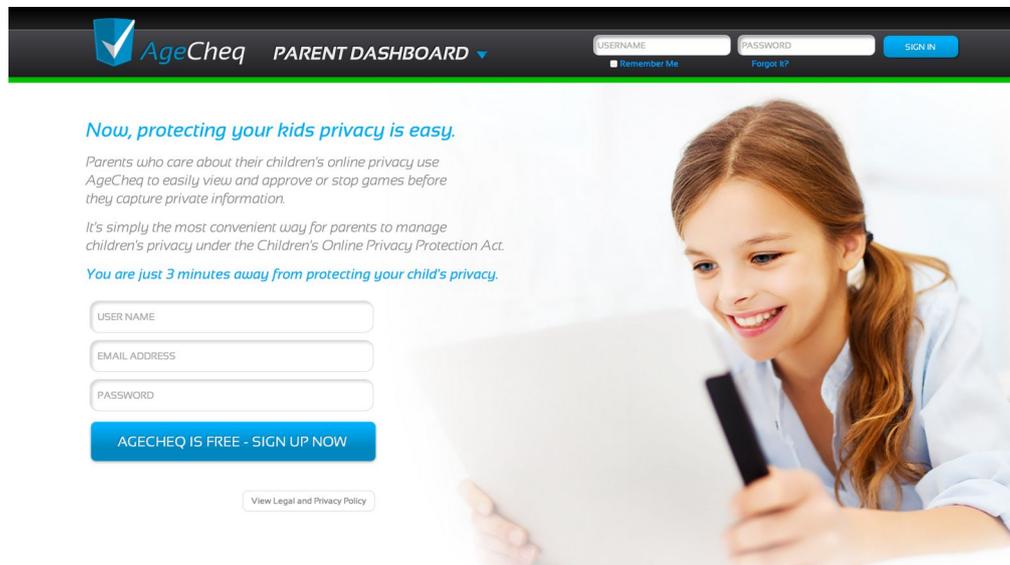
Inclusion of an “approve everything” button

There is no clear rationale for the inclusion the “approve everything” functionality. It appears to perpetuate non-compliance with COPPA by enabling one to forgo providing consent. It is confusing to parents because the service is put forward as method of protecting the privacy of their children – not adults.

There is no reference to this functionality within the legal and privacy policy and no disclosure on its website or materials supporting its inclusion. It would appear that the method as implemented by its sole operator (AgeCheq), leads to a product that is systematically defective without adequate disclosures because this functionality renders the product defective.

Absence of safeguards to reduce the threat of inappropriate developer behavior creates a false sense of assurance for parents

As per the screen shot below all “call to action” made to parents is on the basis of furthering their child’s well being. Comments such as “parents who care about their children’s online privacy use AgeCheq” imply that parents who do not use its service do not care about their child’s privacy.



Further claims that AgeCheq is “the most convenient way for parents to manage children’s privacy” are unsubstantiated and are not supported by any objective assessment. It is likely given the complexity of the product that an ordinary consumer would need omitted information to evaluate the product or service.

The statement that “You are just 3 minutes away from protecting your child’s privacy” is misleading to parents because participation in AgeCheq offers no such protection. AgeCheq by its own definition is a clearinghouse for privacy policies. It does not protect children because it relinquishes all responsibility for privacy protection to developers. It asserts that privacy protection adherence is the responsibility of developers with no clear internal control mechanism to ensure that developers adhere to the privacy policies parents have accepted.

It states that “developers are responsible for incorporating the RCCM into their app and ensuring that approval or rejection responses received from the RCCM are responded to appropriately (by unlocking the app or leaving it blocked)”, suggesting scope for circumvention and diminished acceptance of responsibility.

AgeCheq appears to make multiple claims that it cannot support operationally or technologically, in order to win custom and trust of parents.

False oral and written representations

Extraction of parent address details and date of birth on a false representation

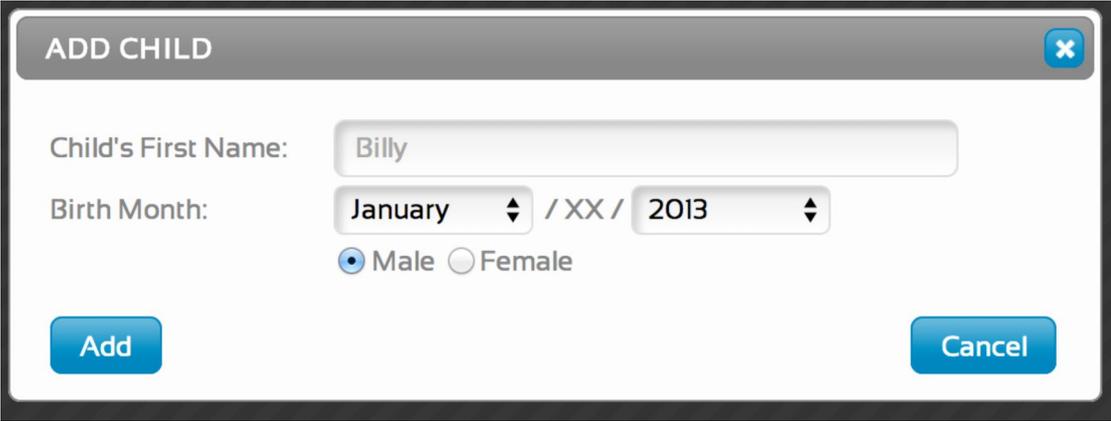
AgeCheq asks a parent for their address birth data when completing a credit card payment for the purpose of verification but does not use the information for the purpose of processing the transaction or mitigating fraud risk.

To test this assumption the researcher, using a fictitious address that did not pertain to the card, completed a transaction to complete the verification process. The transaction was process successfully and the account “verified”.

The point then, is that AgeCheq collects consumer data under a false representation that it is used for compliance. It appears that AgeCheq may capture this data for marketing purposes and the sale of parent data (aggregated or otherwise). This poses a risk to consumers’ personal information.

Unnecessary collection of child data

Under the method as implemented by AgeCheq a parent is required to provide the birth month and year of their children. Screen shot below.



The screenshot shows a dialog box titled "ADD CHILD" with a close button in the top right corner. The form contains the following fields and controls:

- Child's First Name:** A text input field containing the name "Billy".
- Birth Month:** A dropdown menu showing "January", followed by a slash and "XX", another slash, and a year dropdown menu showing "2013".
- Gender:** Two radio buttons labeled "Male" (which is selected) and "Female".
- Buttons:** A blue "Add" button on the bottom left and a blue "Cancel" button on the bottom right.

These details have no evident purpose for inclusion. A parent could link a device based on first name alone. It is not clear whether or not these details are provided to developers / apps linked to the RCCA but it would appear that having obtained parental consent, an operator is free to collect any PII in accordance with that consent – not PII consistent with this information.

If these details are provided to developers / apps linked to the RCCA then it highlights the issue that 93% of device access by children is shared and that the developer would have details of a child that was not in fact the child it was collecting PII from during the participation of its online service.

It appears to be a further occurrence of AgeCheq collecting more data than required in order to complete its process, with no clear indication as to why it needs this data or how it is used; potentially for marketing purposes. In any event the unnecessary data collection poses a risk to consumers' privacy.

Misrepresenting the products and services accessible through use of AgeCheq

AgeCheq implies through imagery on its website that there are specific apps available to users subsequent to registration and verification but none of the apps AgeCheq displays could be found with an AgeCheq authentication mechanism.

There is no statement that these are for illustrative purposes only and the misrepresentation could alter the decision of parents on participation, as they proceed to pay for the service to find no such usability. Screen shot below.



Amazon Web Services (AWS)

AgeCheq, the sole provider of the proposed method, uses Amazon Web Services (AWS). It is accepted that in order to exploit economies of scale and flexibility of provisioning, cloud services are economically attractive to operators. In principle there is no issue with the utilization of the AWS's solution, provided the corresponding security controls are employed and there is an adequate mechanism to monitor and respond to threats in real time.

It is expected as a minimum, that AWS - VPC (virtual private cloud) is utilized. Further that each of any component part of the PII data should be encrypted at work and at rest. Other security controls such as utilizing strong access controls should follow. In addition, the storage and movement of duplicate data must not be less protected than the primary data as described above.

The level of security and controls implemented by AgeCheq is unknown and therefore cannot be commented on directly. However, failure to use the appropriate cloud service with corresponding controls would pose a risk to consumer's personal information.

'Cloud' deployments are widely regarded as vulnerable to the attack of large-scale databases (containing PII) compared to conventional IT infrastructure deployments. This is often a matter of perception, not actuality. Nonetheless, appropriate implementation is imperative because parents were uncomfortable with use of AWS when used by InBloom, the not-for-profit K-12 education technology company backed by the Gates Foundation and Carnegie Foundation.

If adequate controls and safeguards are in place, use of AWS is reasonable.

4. Further matters relating to practices carried out by AgeCheq that are inconsistent with the FTC Mission and Strategic Goal.

Use of bait and switch techniques in conjunction with misleading price claims

Bait-and-switch is a form of fraud used in sales where customers are "baited" by merchants' advertising products or services at a low price, and subsequently pressured to consider higher priced items ("switching").

It is emphasized on the AgeCheq home page that "It's **100% free** for parents".



<http://www.agecheq.com/>

It is emphasized on the parent webpage – provided specifically for parents – as opposed to general audience as in the case of the home page – that “The AgeCheq service is **completely free** for parents”.

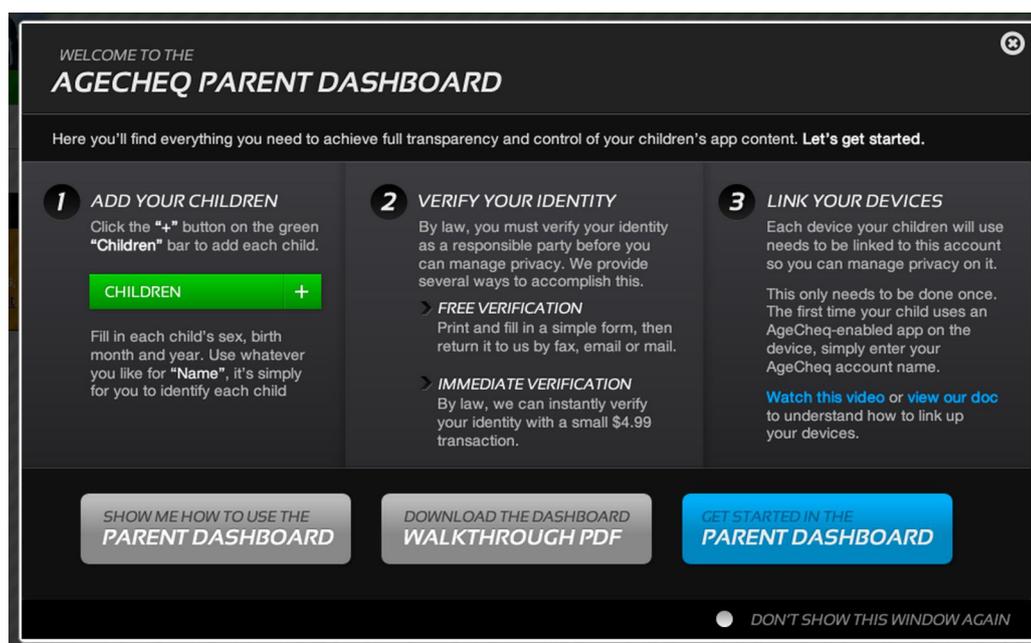
The AgeCheq service is completely free for parents. Sign up now and you'll be all set to view Privacy Disclosures for your childrens' apps.

http://www.agecheq.com/?page_id=10

Only after a parent has registered with a Username, email address and password does AgeCheq state to parents that the account must be verified to be used. The way in which it does so equates to what appears to be gross misrepresentation.

AgeCheq states, “By law we can instantly verify your identity with a small \$4.99 transaction”. There is however no legal requirement for the enumerated method of verifiable parental consent, by monetary transaction, to apply of fee of \$4.99. **AgeCheq appears to use the construct of COPPA compliance and a law, to extort consumers.**

Screen shot provided below.



It is questionable that AgeCheq applies a \$4.99 fee to parents for the “Immediate Verification” but no fee to “print-and-sign” because the cost of processing the manual method would in all likelihood be greater than the processing of a credit card transaction. This appears inconsistent with the FTC “Strategic Goals”, specifically “Protect Consumers: Prevent fraud, deception, and unfair business

practices in the marketplace” because the only information viewable prior to registration states that “the AgeCheq service is completely free for parents”.

It appears that AgeCheq provides “print-and-send” free of charge to support claim that the service is free, in the knowledge that the method is inconvenient for parents, such that it will generate revenues through monetary transactions. If this were not a bait and switch scenario, consumers would expect no fees based on the representations before signup. If there were to be multiple options where some are paid and others free, fees should represent the cost of processing the identity verification and should not use the a false representation of a legal requirement combined with convenience to extract money from consumers.

The cost of processing the credit card payment would not be \$4.99; when accounting for this transaction, US GAAP would require consideration to be allocated to elements of a transaction i.e. allocation to the cost of processing the credit card transaction with the remainder presented as revenue. It is wrong for AgeCheq to assert that its service is free, when there is a charge that charge far exceeds the cost of payment processing and would be recorded as revenue.

Organizations such as Microsoft and Nintendo use a monetary transaction method and charge a nominal amount of \$0.50 – with donations to charity. The approach taken by AgeCheq is inconsistent with industry norms.

Use of the switch and bait technique causes consumers harm. This can be inferred from commenter Sanders under submission #00004 who concluded “Agecheq's website seems very spammy. When I logged in, it asked me for \$4.99 to verify my account as an adult with a credit card”.

Although payment of \$4.99 is inexpensive, the nature of the service being both new to consumers and a proposed solution to complex privacy legislation means that consumers cannot easily evaluate the product and or stated legal requirement to pay for \$4.99. There being approximately 52 million parents online in the U.S. alone means that the amount is material.

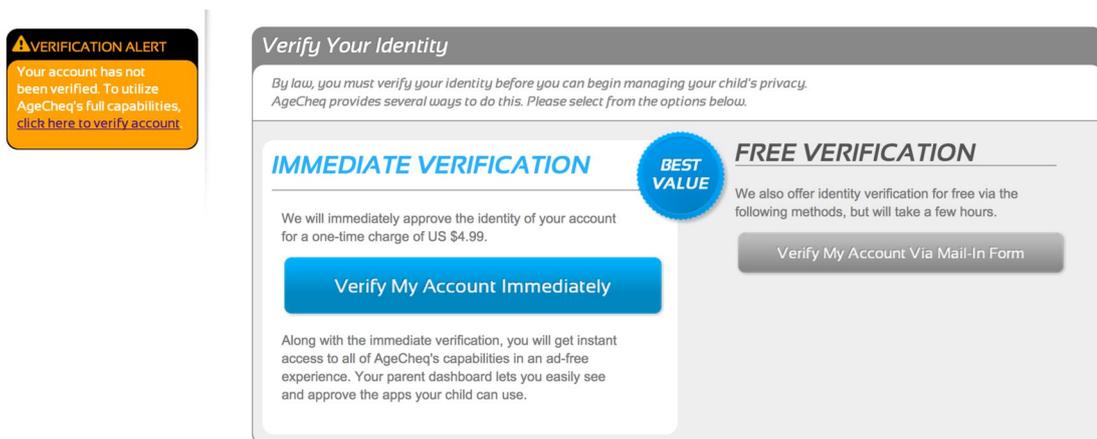
Parents would not know that a payment of \$4.99 is not required for adherence to U.S. privacy law. The product is not frequently purchased and the payment processed on a one-time basis. As such there is no market incentive for the operator not to act in a manner that would reduce the likelihood of repeat purchase, such as carrying out a bait and switch technique.

By the time a user is presented with the misrepresentation that is a legal

requirement for \$4.99 to be charged, the parent has already invested time in the process, Age Cheq is thus more likely to secure a conversion to a paying customer, completing the “switch” under the bait and switch strategy.

Unsubstantiated claim of “Best Value” with no basis for a consumer to compare

A further factor in the analysis of what appears to be a bait and switch technique is the clear prioritization of the credit card verification method using font color, size prominence and an unsubstantiated claim that it is best value for parents.



The presentation both graphically and omission of information made available to consumers to reasonably compare the two methods, indicates that AgeCheq pushes or pressure sells, the method that generates a highest margin. The omission does not enable consumers to determine what is best for them.

In the absence of information for consumers stating the contrary, one would presume that with the free verification, upon completion of the verification process, a parent would get access to all of AgeCheq’s capabilities in an add-free experience – unless AgeCheq intends to generate revenue through targeted advertisements to parents in accounts that are verified by “print-and-send”.

If AgeCheq intends to present advertising to parents alongside child privacy disclosures and the app approval processes, it is reasonable to suggest that this would detract from a parent’s focus when interpreting the privacy information and operator requests to engage with a child. This is somewhat counter to what the service is intended to be – a mechanism to supporting the FTC, COPPA legislation – supporting parental oversight of child privacy.

Reference to “utilize AgeCheqs full capabilities”

As per the screen shot above AgeCheq states that “to utilize AgeCheqs full capabilities, click here to verify your account”. This is misleading because it suggests a freemium type model where a basic level of functionality is provided for free. There is however no subordinate version of a parental consent service without completing identity verification but AgeCheq does not make reference to the necessity to verify identity or make a payment within its sign up flow before registration. Again, this is likely to enhance its new user conversion rate.

Other matters

Defining PII in a manner that would alter consumer behavior where the product does not mitigate but rather exacerbates the alleged threat

In the “Learn more about how AgeCheq works” video AgeCheq provides a definition of COPPA. http://www.agecheq.com/page_id=10

“If you don’t know what the FTC means by Personally Identifiable Information or PII, it is the little bits of information that when collected all together could lead a sinister actor back to an individual kid. This information may seem anonymous and harmless at first but when aggregated together it could reveal a whole lot of sensitive information about your child”.

Andrew Smith, Director of Developer Education at AgeCheq

This compares to the FTC definition

<http://www.coppa.org/coppa.htm>

(8) PERSONAL INFORMATION.—The term "personal information" means individually identifiable information about an individual collected online.

<http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions>

The amended Rule defines personal information to include:

First and last name;

- A home or other physical address including street name and name of a city or town;
- Online contact information;
- A screen or user name that functions as online contact information;
- A telephone number;
- A social security number;

- A persistent identifier that can be used to recognize a user over time and across different websites or online services;
- A photograph, video, or audio file, where such file contains a child’s image or voice;
- Geolocation information sufficient to identify street name and name of a city or town; or
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above.

This choice of definition and use of the phrase “sinister actor” appears to be another use of aggressive sales techniques intended to worry and intimidate parents into becoming users of AgeCheq. Although one would not necessarily expect a verbatim recital of the FTC definition it could be put in layman’s terms in a clear concise way, for parents to form an objective, unimpaired interpretation.

Use of the word sinister, in conjunction with the misrepresentation that AgeCheq protects children and its false implicit message that AgeCheq reduces the level of PII an operator could collect to behave in a sinister manner, may lead consumers to make a purchasing decision that they otherwise would not have, if provided with all of the information required; free from the above misrepresentations.

Appointment of Bob Teufel to the Board of Directors

The addition of Bob Teufel to Board of Directors in April 2014 confirms the intention that AgeCheq will generate revenue from marketing activities that it has not adequately disclosed to parents and increases the seriousness of the shortcomings in its implicit privacy policy acceptance and free-reign to modify.

As per the news release – <http://www.mobilitywire.com/agecheq/2014/07/09/8439>

“Bob Teufel, the retired President of Rodale Inc., brings a wealth of publishing and direct marketing experience to the AgeCheq board of directors, having served Rodale for nearly 40 years. He has served as chairman of the Direct Marketing Association (where he is also a member of its hall of fame), the Magazine Publishers of America, the American Magazine Conference and the Magazine Congress.

During his tenure with Rodale, Bob is credited with creating the concept for Men’s Health magazine, establishing Prevention as the top consumer well-being publication in the country, producing The Doctors Book of Home Remedies, which has sold more than 20 million copies worldwide, and taking Rodale’s annual sales from \$60 million to more than \$500 million.

Bob most recently served on appMobi's board of directors, advising the mobile app development platform company towards its eventual acquisition by Intel. With a long history of directing firms within the mobile app industry and proven leadership skills within the field, Bob brings crucial insight and guidance as AgeCheq continues to expand".

appMobi engages in "cross platform push messaging, app promotion, in-app purchasing, integrated analytics and more, for all applications and deployed in any environment". <http://www.appmobi.com/>

This inclusion of this reference to Bod Teufel is not intended to be defamatory. Mr Teufel has had a career of exceptional achievement and only recently joined the AgeCheq management team. The reason for its inclusion is solely on the basis that the strategic hiring of an expert in revenue generation through marketing, makes AgeCheqs' intentions for its management of consumer PII very clear – that is to sell the data and present them with marketing – the disclosures for which require no acceptance or conscious participation and can be changed by AgeCheq at will. It is clear that the proposed method and more specifically the applicant, puts consumers' personal information at risk.

App only suitability

AgeCheq asserts (when contacted) that it has SDKs that make it suitable for use by websites as well as smart device apps however references made by Mr Smith in the submission suggest the AgeCheq is for mobile only.

"The mobile app industry requires a single, simple-to-use system that manages COPPA compliance for both publishers and parents, and that is exactly what AgeCheq is."

Roy Smith, Founder and CEO

There is insufficient information in the public disclosure to comment on this, suffice to say that one should reasonably expect any newly approved method to be applicable both on websites and apps.

Device must be owned

It is unclear how AgeCheq would work with desktop devices and or smart devices that are not owned by the child e.g. a public access device such as library hardware or school owned hardware. Less affluent families that rely on public services would appear to be socially excluded by the proposed method.

Conclusion

The method does not meet the requirements of 16 CFR 312.5(b)(1) and poses a risk to consumers' personal information. The manner in which the method is presented creates a false sense of assurance to all parties and would appear to create more harm than benefit. Existing enumerated methods and other general parental consent platforms provide a higher assurance level.

AgeCheq is the sole operator of the method and appears to engage in practices that conflict with the FTC, such as bait and switch techniques, misrepresentations and omissions. Approval of the method would be counter to the FTC Strategic Goal to protect consumers and its Mission to prevent business practices that are unfair to consumers.

Approval of this method could lead to social exclusion that would disadvantage underprivileged children.

Caveat

In the event that there is further information provided by AgeCheq to the Commission but redacted, that would enable a contrarian view to be formed, I respectfully propose that in light of what appear to be significant potential threats to the privacy of consumers, this information is put forward for public comment on the basis of public interest.

In the absence of full disclosure by AgeCheq and not being party to the decisions to implement the method and certain features within the AgeCheq service more broadly, the critique in this submission is limited to observation, user testing and inference. Comment has not been sought from AgeCheq management.

References

References included where pertinent. Full referencing available where required.

<https://www.common sense media.org/research/zero-to-eight-childrens-media-use-in-america-2013>

<https://www.cia.gov/library/publications/the-world-factbook/rankorder/2127rank.html>

<http://www.theguardian.com/technology/2014/jun/03/facebook-children-join-social-network>

http://www.fbi.gov/news/stories/2011/may/predators_051711/predators_051711

<http://www.nsopw.gov/en/Education/FactsMythsStatistics>

<http://www.bjs.gov/content/pub/pdf/vit12.pdf>

<http://www.lowcards.com/dummies-guide-to-credit/credit-card-statistics>

<http://www.experian.com/live-credit-smart/state-of-credit-2013.html>