

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

December 24, 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-155400

This document responds to the FTC request for public comment.

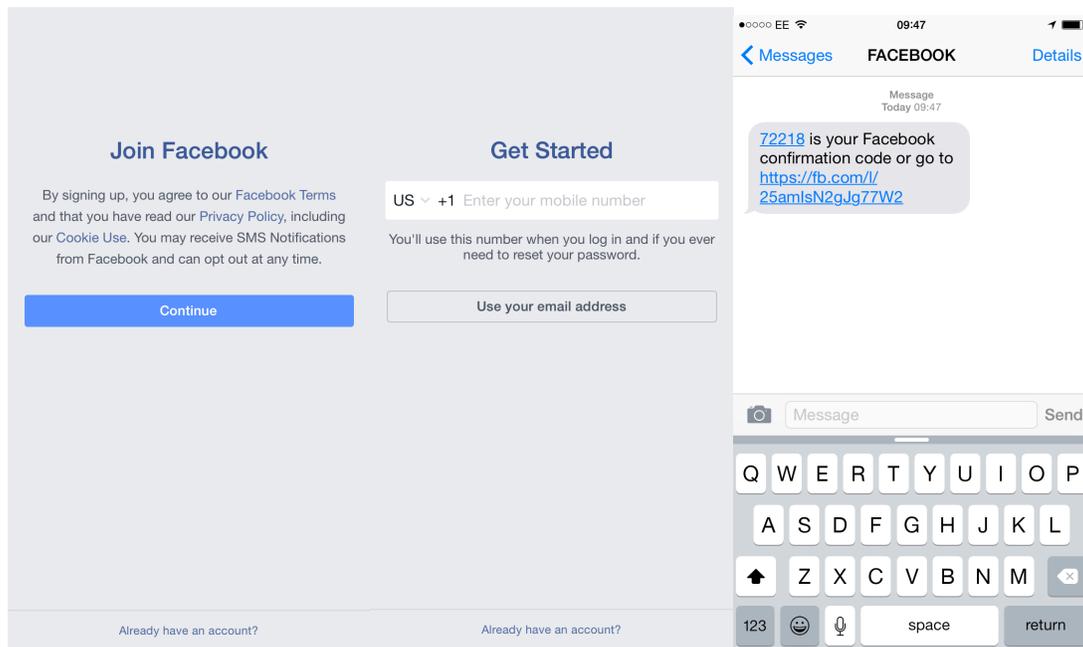
- 1. Does the proposed method, both with respect to the process for obtaining consent for an initial operator and any subsequent operators, constitute a new methodology or is it already covered by existing methods enumerated in § 312.5(b)(1) of the Rule?*

The proposed method does constitute a new methodology because it is not already covered by existing methods enumerated in § 312.5(b)(1) of the 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 Device-Signed Parental Consent Form (DSPCF) methodology does not meet the requirements for parental consent laid out in 16 CFR 312.5(b)(1). Specifically, the method is not reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent or even an adult.

Social networks such as Facebook use the core component of proposed DSPCF method (a text message and verification code) in their user registration flows.



In its rejection letter to the President of AssertID the Commission stated; “commenters note that users can easily fabricate Facebook profiles, and in fact, Facebook’s own 10-Q filing with the Securities and Exchange Commission indicates it has approximately 83 million fake accounts, which represents about 8.7% of its users. Second, one comment highlights the fact that children under 13 have falsified their age information to establish social media accounts, including very active accounts with significant age-inflation that could appear to be credible”. The social graph and its reliability – concluded as inadequate by the Commission – is based on the verification of the users using the AgeCheq DSPCF method and the social graph is essentially a proxy it. To that extent, the Commission has already rejected the method proposed by AgeCheq.

It is acknowledged that the DSPCF method includes the addition of a digital signature however, as the applicant states, the Commission has previously remarked that despite public comments encouraging the use of digital signatures, the term "digital signature" was overly broad and "without more indicia of reliability, were problematic in the context of COPPA's verifiable parental consent requirement”. Therefore, whilst acknowledged, the digital signature has already been concluded as inadequate in the absence of an additional process that increases its effectiveness. As evidenced here, the applicants Device-Signed Parental Consent Form is not an adequate addition.

AgeCheq makes the unsubstantiated assertion that its method is credible because the text message would be sent to a device that a parent owns, pays for and controls. AgeCheq asserts that it is fairly presumed that parents of children under 13 years of age have physical access and/or physical control of the device on which the child is accessing online services. The assertions indicate that AgeCheq is not to be knowledgeable about prior COPPA violations; which is further demonstrated by the inadequacy of the DSPCF method. For the benefit of AgeCheq, in March 2014 the Commission approved a final order resolving FTC allegations that Apple Inc. unfairly charged consumers for in-app purchases incurred by children without their parents' consent. Apple was ordered to provide full refunds to parents, totaling a minimum of \$32.5 million with any remaining balance not refunded remitted to the commission. Apple allowed children to make purchases within a 15-minute period after a parent gave explicit consent to make a purchase (having submitted the AppleID of the account on the device). This implicitly demonstrates that there are recurring time periods of at least 15 minutes during which a parent cannot be assumed to control a device, be it their own or their child's; even if they pay for it. In making its final order in relation to Apple, the Commission has publicly disproved the assertions made by AgeCheq, which are critical to the DSPCF method.

The proposed method is ill considered and appears to offer a lower level of protection to children and their parents than the email plus method, which of course affords operators a lower level of data permissions than other methods.

The applicant is unable to provide sufficient evidence or even reasonable assurance that the method is effective. The applicant draws a parallel with a general audience communications product that uses a text message verification code system to verify the phone number of the user, not to verify identity to the extent required in order to obtain verified parental consent.



Verifying your phone number in WhatsApp

WhatsApp uses your phone number to make chatting with friends and family easy. This way, you don't need to remember usernames or accept any friend requests. The phone number verification process is designed to be as simple as possible, but if you are having trouble verifying your number, please be sure to check the following:

The DSPCF method should be rejected.

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?*

The proposed method poses a risk to consumers' personal information – specifically children because AgeCheq has no credible means of ascertaining that a parent, or even an adult provides consent. Given that AgeCheq further suggests that the method is used by intermediaries to provide what is effectively a blanket consent to operators, the risk and threat to the privacy and digital safety of children is high. The risk to consumers' personal information benefits businesses and more specifically AgeCheq, to the detriment of consumers and is not outweighed by the benefits of using this method.

Conclusion:

The method does not meet the requirements of 16 CFR 312.5(b)(1) in light of available technology and poses a risk to consumers' personal information. Existing enumerated methods known to the market provide a higher assurance level.

AgeCheq appears to lack knowledge of prior parental consent methods rejected by the Commission and the Apple violation, which collectively disprove the technology and assumptions that are critical to the DSPCF method and demonstrate its inadequacy. The result is an ill-considered proposal.

Approval of the method would be counter to the FTC Strategic Goal to protect consumers. The DSPCF method should be rejected.

Review of the AgeCheq submission (verbatim) in the form of excerpt followed by comment.

Excerpts from the AgeCheq submission are in red font.

Comments made and content included by Tom Strange are presented in bold font.

The intermediary transmits a validation code via text message (or automated voice call) to that number, which the parent enters into the online "sign and send" type form and transmits to the intermediary to complete the verification process;

Recognizing that the perfect should not be the enemy of the good, many methods which

pose some risk of evasion by a child have been deemed sufficiently reliable as a matter of law, including signing and sending a paper form by mail, fax, or scanning/emailing. **Indicates acceptance of method inadequacy, drawing comparison to methods enumerated in 1998 as opposed to subsequently enumerated methods and a review of the methodology in light of available technology as of 2014.**

The proposed digital/mobile verification method materially improves on basic digital sign and click authentication (rejected by the Commission in the Final Rule6) - by relocating the signature collection to a neutral third party intermediary (as opposed to the games/sites themselves) - where the parent must register, and then (most importantly) logically ties a digital signature to the mobile telephone used by the parent. **The DSPCF does not improve on digital sign and click it simply exacerbates the risk because the flawed process is completed only once, for all operators that integrate with the intermediary. It ties the signature to a phone but there is no way of knowing that it is the device used by the parent or a shared device to which a parent consents.**

2) The parent completes an onscreen form with personal information (minimally name, address, birth year, and mobile telephone number)

A child could provide all of this information, unlike knowledge-based-questions where the likelihood of process completion is significantly reduced.

3) After the parent has submitted their personal information, a validation code is transmitted to the parent's mobile telephone.

There is nothing at all to substantiate that the verification code goes to a parents phone - as opposed to the child's own phone.

4) The intermediary then displays an onscreen form that requires the parent to enter the validation code just received on the mobile telephone.

At no point has an identity been verified such that there can be reasonable assurance that the person providing consent is the child's parent.

5) The parent digitally signs the certification on the screen.

Any one could do this - child or otherwise

6) The parent then touches or clicks an onscreen button to indicate their acceptance of the signed identity declaration.

Neither signing the form or acceptance of a declaration constitutes verification. Neither are they an adequate deterrent to circumvention.

In its reasoning for not including digital signature in the list of approved parental consent mechanisms, the Commission expressed concern about the ease with which a child could circumvent a simple digital signature, saying "simple digital signatures, which only entail the use of a finger or stylus to complete a consent form, provide too easy a means for children to bypass a site or service's parental consent process" (i.e., to

"instantly pen and send a signature")

The Commission has already concluded that use of a signature alone is inadequate. The question then, is whether or not the addition of a text message verification code system brings the method to an acceptable level. This report finds it does not.

Children are less likely to encounter the form. Children frequent the operators' sites- the online services themselves, such as a game to be played on a smartphone or tablet. They are not as likely to locate, register and log into the intermediary website, nor to complete the necessary online registration (which includes neutral age screening in any event)

That children are less likely to encounter the form is conjecture. Numerous factors would impact how likely it is that a child would find the intermediary e.g. brand and service recognition within groups of parents and children, SEO and paid marketing campaigns. Inclusion of this point by AgeCheq implicitly acknowledges that a child could circumvent the verification process if located on an operators website. Given that AgeCheq accepts a child could circumvent its multi-step digital process in an illicit registration, it is reasonable to suggest that a child would find an intermediary website i.e. AgeCheq. There is no justification to the claim that this additional step is a barrier. No credence can be given to this claim.

Parents of children under 13 years of age are fairly presumed to have physical access and/or physical control of the device on which a child is accessing online services, which collect personal information from the child, or the device.

Again this is conjecture. Available evidence indicates that parents do not have physical access to a device and or physical control of a device on which a child is accessing online services to the extent necessary to ensure that the parent is in receipt of the confirmatory text message and party to the consent process. Reference Apple fines.

The validation code step transmits a text or automated voice message to this device (which may be the parent's own phone, a shared device, or the child's own device if one posits the "child bad actor" who is evading parental involvement). The mobile phone's text message inbox will show the date and time of the reception of the validation code, and the validation code itself. (Alternatively, a parent could elect to receive an automated voice message, which also would leave behind evidence of the transaction).

This process provides no further verification that the person providing consent is the parent than the method of parental consent by email plus i.e. there is no enhanced assurance that the cell phone number provided is that of the parent as opposed of being that of the child, just as is the risk in the email method.

There is in fact lower level of assurance than email plus because parents may have access to their child's email accounts (if they provided them with one) on their own mobile devices via IMAP, where as the child's mobile phone number is linear and the channel of communication between the child and other party by text message cannot easily be monitored.

There is no mechanism preventing the deletion of a text message from the inbox of the mobile phone and no mechanism for identifying where a message has been deleted. Neither is the manner in which a message is deleted sufficiently complex such that a child would be unable to do it.

There is no mechanism preventing the deletion of a text message from the inbox of the mobile phone and no mechanism for identifying post deletion that a message has been deleted. Neither is the manner in which a message is deleted sufficiently complex such that a child would be unable to do it because it is designed to be a simple user experience. Taking iOS8 as an example, one touch on a message opens the message and one swipe across the message deletes it – there is no reliable audit trail.

Logically tying the device to the consent form is itself a strong additional indicator of reliability beyond the digital signature itself.

Tying a device to the consent form provides little to no additional reliability when attempting to ensure that the person providing consent is the child's parent there is a high probability that the device tied to the signature is not that of the parent and there is no way of detecting false positives.

The multi-step process (which involves entering the correct mobile telephone number, having physical access to that device, and entering a validation code) is much more reliable than merely having an operator collect a "pen and send" digital signature.

This taken collectively with the following:

The above process is harder to evade than the "sign and send" paper form method originally approved and widely used for many years (without even anecdotal evidence of a pattern of evasion by children under 13, as was noted in the rule making proceedings leading to the Final Rule). With the paper form, the parent gets no record that a transmission or mailing ever took place. The hypothetical "child forger" (again, a remote and never documented pattern of misuse) can print and mail/email a form in secret.

The multi-step process creates the appearance of being more reliable than “pen and send” more commonly referred to as the “print-and-send” method because it uses a mobile device, creating the impression of technological innovation. However, the provision of a signature is the same whether on a printed form or on a mobile device. The question then is which method – printing and scanning / faxing / posting a form vs. a code in a text message – is least likely to be circumvented. In view of the high friction involved in “print-and-send” and multiple steps required, it could be reasonably asserted that children are less likely to engage in the process and effort required to circumvent the “print-and-send” than the DSPCF. Moreover the “print-and-send” method is not commonly implemented by operators; they typically opt for

social security numbers or credit card transactions. As a third point, the Commission added to its list of available methods, the use of knowledge-based questions, which is more rigorous with a lower scope for circumvention than the DSPCF proposed by AgeCheq in this submission. The addition this method to those already approved would represent a backward step in the protection of child privacy online.

After registration, the intermediary will have a digital record that at a certain date and time, someone using, for example, mobile telephone number 555-555-1212 provided a correct validation code, name, address, birth year, and the digital image of the signature.

Taken with the following comment:

The intermediary, for its part, would have a digital record that at a certain date and time, someone using mobile telephone number 555-555-1212 provided a validation code, and the identifying information fields, as well as a digital image of a signature. This record could be provided to parents after the fact, which is a significant advantage over the paper sign and send method.

This process may provide an operator with an audit trail that could be provided in the event of a Commission enquiry but does not act as a mechanism to enhance the likelihood that the person providing consent is the child's parent. It is highly unlikely that a parent would proactively contact a company such as AgeCheq, which implements the proposed method in order to query whether or not their details have been provided for the purpose of completing a consent process – neither should parents be expected to do so. The applicants comment therefore adds no value in the context of consent efficacy. The keeping of historic records for audit purposes by an intermediary cannot be expected to mitigate the risk of a person other than the child's parent providing consent.

The test for reliability should be whether the method is at least as reliable as the previously enumerated methods, for these methods have satisfied the statutory requirement for a "reasonable effort" as a matter of law.

The applicant appears not to appreciate the process in which it has submitted this application and the standard to which the method must be assessed. The commission states clearly that any proposed method must be assessed as to whether or not it is reasonably calculated, in light of available technology. The applicant appears to request comparison against technology available when the Rule was drafted more than 15 years ago. This is disconcerting in terms of AgeCheq understanding of COPPA.

With a registered mobile device included in the process- a device which a parent owns, pays for, and controls-the parent would receive actual notice after the fact of the (hypothetical) child "bad actor" having transmitted a forged signature.

The applicant has no means of providing assurance that the number associated with a device, to which the text based message complete with verification code is sent, is owned, paid for or controlled by a parent. Even where there is ownership and payment there is commonly not control – hence the Apple fine for in-app purchases without parental consent – there was an absence of control.

Many mobile applications where connecting a device to an authenticated identity, such as WhatsApp or Pango, rely on a register/validation code process. A digital signature coupled with device-based validation (and transmittal of confirming messages) is widely used commercially today. In short, the proposed method represents a more than "reasonable effort" that is materially more reliable than other methods already deemed adequate as a matter of law.

The applicant appears to believe that the use of the proposed method by Whatsapp is sound basis for it being approved for COPPA compliance but Whatsapp does not use the method for verification of identity or a consent process. Whatsapp uses it to verify a users phone number, which serves as a proxy to the Whatsapp user profile.



WhatsApp uses your phone number to make chatting with friends and family easy. This way, you don't need to remember usernames or accept any friend requests. The phone number verification process is designed to be as simple as possible, but if you are having trouble verifying your number, please be sure to check the following:

- You have the **latest version** of WhatsApp installed from the [App Store](#).
- You have entered your full [international phone number](#), including the country code (or select your country from the country list).
 - An example of a US phone number is: + 1 408-555-1234.
- Please **omit** any **leading zeros (0s)** or **exit codes** from your number.

AgeCheq presenting Whatsapp and social communications products as an example of evidence that the method is effective demonstrates how ill considered this submission is given the Commission's rejection of the method proposed by Assert ID.

http://www.ftc.gov/sites/default/files/documents/closing_letters/16-cfr-part-312-childrens-online-privacy-protection-rule-commission-letter-determining-assertids/131113assertid.pdf

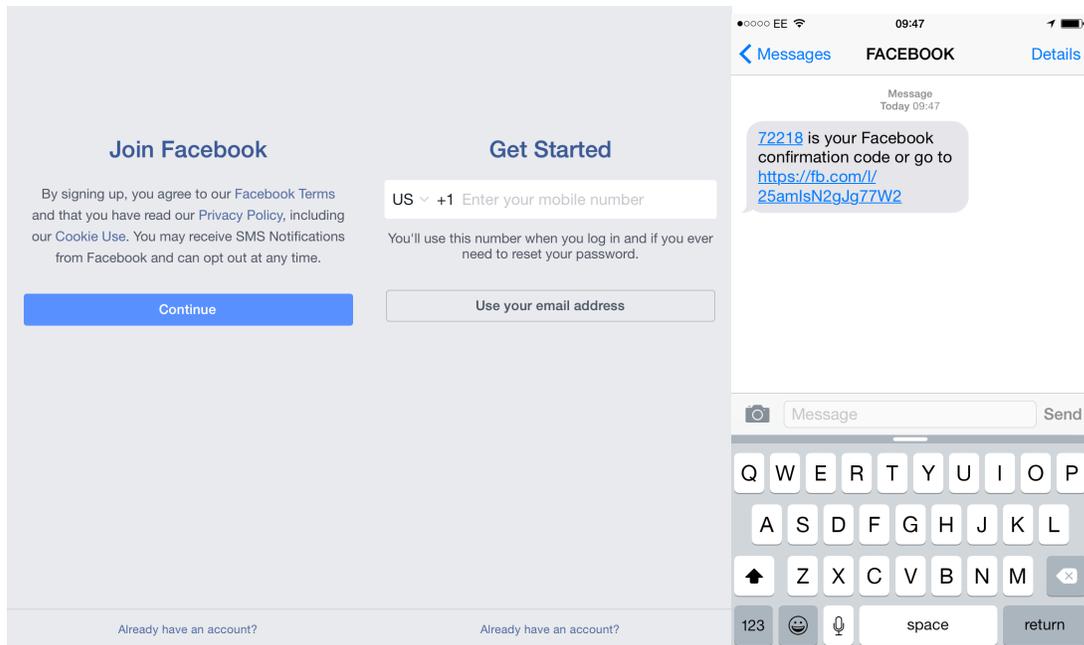
"The Commission has determined that AssertID's proposed VPC method of social-graph verification does not meet the criteria for approval set forth by the Rule.

Specifically, AssertID has failed to provide sufficient evidence that its proposed VPC method is “reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent” as required by the Rule. Without relevant research or marketplace evidence demonstrating the efficacy of social-graph verification and that such a method is reasonably calculated to ensure the person providing consent is the child’s parent, the Commission believes approval of such a VPC method under the Rule would be premature. Although AssertID identified several articles that discuss the general topic of the influence of social networks on trust among their members, none appear to support a claim that AssertID’s social-graph verification is an effective method of verification.

AssertID’s limited beta testing of its product does not demonstrate that social-graph verification will work in a live environment or that the method is reasonably calculated to ensure the person providing consent is the child’s parent.

We are persuaded by commenters’ concerns about the reliability of social-graph verification at this time. First, commenters note that users can easily fabricate Facebook profiles, and in fact, Facebook’s own 10-Q filing with the Securities and Exchange Commission indicates it has approximately 83 million fake accounts, which represents about 8.7% of its users. Second, one comment highlights the fact that children under 13 have falsified their age information to establish social media accounts, including very active accounts with significant age-inflation that could appear to be credible”.

The method submitted by AgeCheq is essentially a proxy for the social graph – already declined – because an individual can use the proposed method to obtain accounts with the social services referenced in the social graph application, specifically Facebook, which has 83 million fake accounts. The social graph was concluded as ineffective, meaning that by default the method proposed by AgeCheq is too.



There is no precedent or reliable evidence substantiating the use of the proposed method for identity verification or consent processing. It has only ever been used to ascertain that the registrant is human (not a computer program designed to complete service registrations and spamming) and to verify a mobile phone number associated with an account. This differs markedly to the previously approved knowledge based questions method which has been demonstrated as an effective method in industries where a high level of certainty is required and is already adopted by credible organizations for that purpose i.e. Lexis Nexis Risk Solutions and its acquisition of RSA Security, Inc.'s KBA technology and credit bureaus, such as Experian (which markets its own KBA product).