AgeCheq

Donald S. Clark, Secretary
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
Via Hand Delivery

October 1, 2014

Re: Application Pursuant to Section 312.12(a) of the Final Children's Online Privacy Protection Rule for Approval of Parental Consent Method Not Currently Enumerated in §312.5(b)

Dear Mr. Clark:

Pursuant to Section 312.12(a) of the Final Children's Online Privacy Protection Rule (the "Final Rule"), AgeCheq Inc. ("AgeCheq") hereby requests Federal Trade Commission ("Commission") approval of a parental consent method not currently enumerated in the Final Rule. The method is truly innovative and provides an additional useful parental verification method uniquely suited to the mobile devices and applications which today's parents routinely make available to children under 13.[1]

Please note that this application is submitted independently of AgeCheq's pending application for Commission approval of a parental consent method not currently enumerated in the Final Rule.[2]

AgeCheq is a technology services company specializing in cloud-based privacy management services for mobile devices, websites, and desktop computers. AgeCheq offers a suite of compliance

[1] *See* FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing* (Feb. 2012), at 1 n.6, available at http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

[2] *See* #579: 16 CFR Part 312: Children's Online Privacy Protection Rule Proposed Parental Consent Method; AgeCheq Inc., Application for Approval of Parental Consent Method, No. P-145410 (August 25, 2014).

services to operators of websites and online services, but particularly to mobile game and app publishers,[3] including those whose activities are ad-supported.

The proposed "Device-Signed Parental Consent Form" ("DSPCF") method adapts the currently enumerated (paper) "sign and send" parental consent method to the mobile ecosystem, in light of the Final Rule's extension of the Children's Online Privacy Protection Act ("COPPA") to mobile applications and smartphones and tablets, as follows:

- A third party intermediary[4] has an online verification portal, accessible to parents on the world wide web or otherwise;
- The portal presents an online "sign and send" type form that collects the parent's mobile telephone number among other identifiers;
- 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; and
- The intermediary stores the consent record on behalf of the operators and parents.

BACKGROUND AND SUMMARY OF PROPOSED METHOD

By statute, the term "verifiable parental consent" means "any reasonable effort (taking into consideration available technology) . . . to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the

[3] *See* AgeCheq Application Pursuant to Section 312.12(a) of the Final Children's Online Privacy Protection Rule for Approval of Verifiable Parental Consent Method Not Currently Enumerated in Section 312.5(b), July 25, 2014, available at http://www.ftc.gov/system/files/attachments/press-releases/ftc-seeks-public-comment-agecheq-inc.proposal-parental-verification-method-under-coppa-rule/140825agecheqapp.pdf. This application is distinct from AgeCheq's July 25 application seeking approval of a real-time common consent mechanism,as a matter of regulatory approval and also as a technical matter, very obviously. The proposed device-based digital signature, if approved, can be integrated with the real time common consent mechanism described in the first application, as a technical matter, delivering a total solution for parents and operators alike, but as a regulatory matter, they are independent, not dependent, proposals.

[4] Alternatively, an operator of a website or online service directed at children under 13 could host and complete this verification process directly, on a website or within an application. AgeCheq believes that the additional indicia of reliability afforded by tying a digital signature to a particular device under parental ownership and control is strong, and meets the statutory requirement of a "reasonable effort" to verify that a parent has actually consented. Having a third party intermediary host and curate that verification process is even more reliable.

collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child."[5] 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.

The proposed digital/mobile verification method materially improves on basic digital sign and click authentication (rejected by the Commission in the Final Rule[6]) 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 proposed method would work as follows:

1. A parent visits and registers at a third party intermediary (such as AgeCheq, but by no means limited to AgeCheq – existing safe harbor approved programs or other new entrants could administer the same process);
2. The parent completes an onscreen form with personal information (minimally name, address, birth year, and mobile telephone number) (See Figure 2);
3. After the parent has submitted their personal information, a validation code is transmitted to the parent's mobile telephone. (See Figure 3). The parent can elect to receive the code by text message, or by a computer generated voice call;
4. The intermediary then displays an onscreen form that requires the parent to enter the validation code just received on the mobile telephone. (See Figure 4). The personal information previously provided by the parent is displayed, along with a statement of certification verifying ownership of the device and the accuracy of information;

[5] 78 Fed. Reg. 3,986 (2013).

[6] *Id*. at 3,988.

5. The parent digitally signs the certification on the screen. The method of signing may vary based on the type of computer the parent is using. It could be done using a computer mouse, stylus or fingertip, as applicable;
6. The parent then touches or clicks an onscreen button to indicate their acceptance of the signed identity declaration;
7. With the parent's assent, the intermediary marks the parent's account as "Parental Identity Verified by Electronic Consent Form"[7];
8. Operators registered with the intermediary can rely upon the stored parental verification when parental consent is sought in future sessions;
9. For implementations that require the ability to audit the parental identification in the future, the intermediary can securely store the captured data, which includes the image of the signed form, the mobile telephone number and parent's personal information; and
10. If there is a need to review the signed form or identity information, the stored DSPCF data can be retrieved, decrypted (if stored using encryption) and reviewed.

[7] Security is a concern and priority whenever personal data is stored. At AgeCheq, for example, such personal data is encrypted and stored in secure cloud storage using AES 256 encryption and dual key HMAC authentication. Moreover, the privacy practices of the intermediary are also germane. At AgeCheq, identifiable information, including the information on the proposed consent form is never shared, and used only for purposes of delivering AgeCheq's COPPA consent and related services.

DESCRIPTIVE FLOW CHART OF THE PROPOSED METHOD

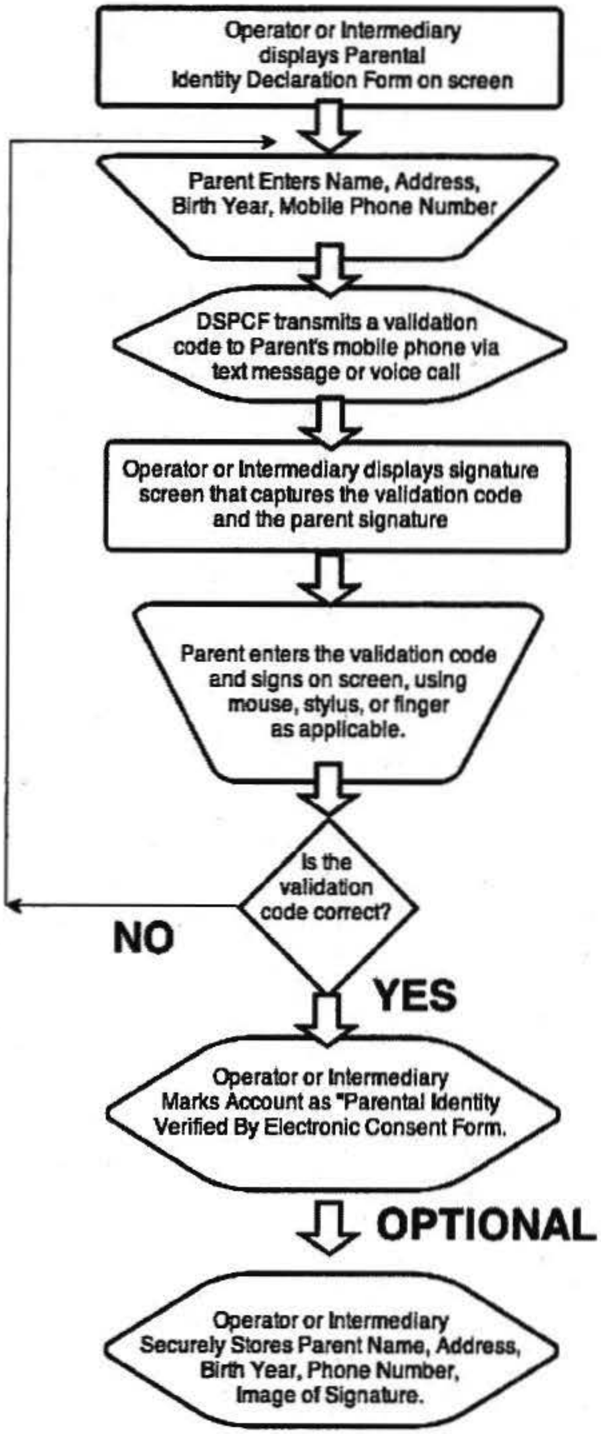

Operator or Intermediary displays Parental Identity Declaration Form on screen
Parent Enters Name, Address, Birth Year, Mobile Phone Number
DSPCF transmits a validation code to Parent's mobile phone via text message or voice call
Operator or Intermediary displays signature screen that captures the validation code and the parent signature
Parent enters the validation code and signs on screen, using mouse, stylus, or finger as applicable.
Is the validation code correct?
NO
YES
Operator or Intermediary Marks Account as "Parental Identity Verified By Electronic Consent Form.
OPTIONAL
Operator or Intermediary Securely Stores Parent Name, Address, Birth Year, Phone Number, Image of Signature.

Figure 1- Descriptive Flow Chart of Typical DSPCF Operation[8]

[8] For a video demonstration of this process, please visit: http://vimeo.com/agecheq/review/105166391/808afb1cf0.

COPPA REQUIREMENTS FOR APPROVAL AS A NEW METHOD

The proposed DSPCF method is not already covered by existing methods enumerated in Section 312.5(b)(1) of the Final Rule. In section II.C.5 of the "Final Rule Amendments" relating to COPPA dated January 17, 2013, the Commission specifically remarked on the potential use of digital signature for parental consent, stating 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.*"[9] Therefore, any method using digital signatures is not among the currently enumerated approved methods.

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. 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").[10] The proposed DSPCF resolves these concerns by adding further indicia of reliability:

- 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);
- 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

[9] 78 Fed. Reg. 3,988 (2013).

[10] *Id.*

personal information from the child or the device. 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.)

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

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 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 rulemaking proceedings leading to the Final Rule[11]). 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. With a registered mobile device included in the

[11] *Id.* at 3,991 n.253 (citing comments suggesting that only a small percentage of children are likely to falsify parental consent.)

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 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.

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 proposed method does not pose a disproportionate risk to consumers' personal information, in light of the benefit to consumers and businesses of using this method. Because the proposed method captures parental identity information, a graphic representation of a signature, and device identity information, this is a valid concern. As a starting point, all methods necessarily involve the collecting and/or storing of personally identifiable parental information, such as telephone number, physical mailing address, social networking accounts, digital image of the parent's signature, Social Security number, or credit card number. The only additional personally identifiable information captured under the proposed DSPCF method are digital identifiers of the parent's device, and as proposed, it is optional for the operator or intermediary to collect and store the digital identifiers for increased security.

On the other hand, the proposed method is innovative, useful, and cost-effective for parents and operators alike.

- It allows parents to conveniently provide verifiable consent using their personal mobile devices;[12] and
- It drastically reduces the cost and complexity required of operators who must get verifiable parental consent under the Final Rule.

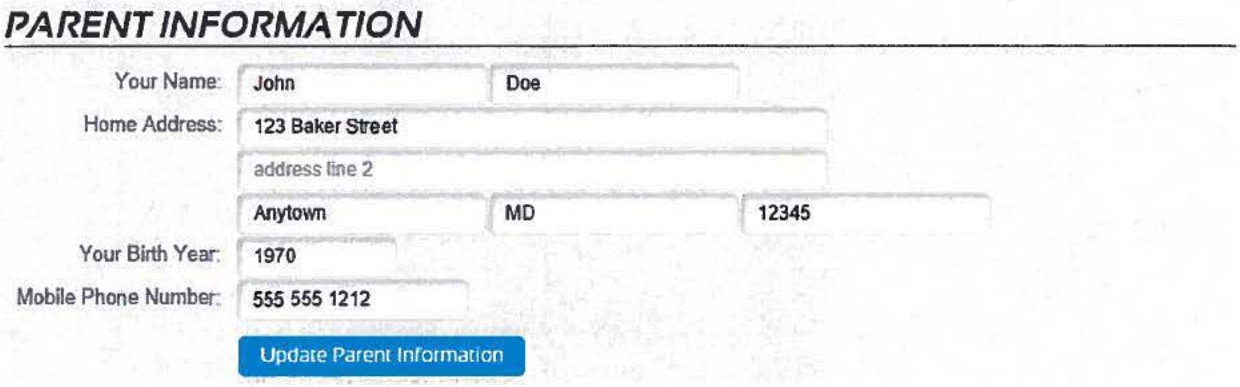
For the foregoing reasons, AgeCheq requests that the Commission act favorably upon this application, made pursuant to 16 C.F.R. § 312.12(a), and approve the proposed Digitally Signed Parental Consent Form as a new method of parental consent.

AgeCheq greatly appreciates the Commission's valuable time and consideration with respect to this application.

Sincerely,

Roy R. Smith II, CEO

[12] *See id.* n.220 *citing, e.g.*, Direct Marketing Association (comment 37, 2011 NPRM), at 23 (Congress passed ESIGN Act over a decade ago and consumers prefer completing transactions online with digital signatures over using cumbersome offline processes); Entertainment Software Association (comment 47, 2011 NPRM), at 22-23 (electronic sign-and-send method meets the statutory standard of 'reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent,' while accommodating parents' use of tablet, mobile device, and small-screen technologies lacking computer peripherals such as printers or scanners); TechFreedom (comment 159, 2011 NPRM), at 8 (urging the Commission to promote development of solutions such as electronic signatures now, rather than wait for the next Final Rule revision).



PARENT INFORMATION

Your Name: John Doe

Home Address: 123 Baker Street

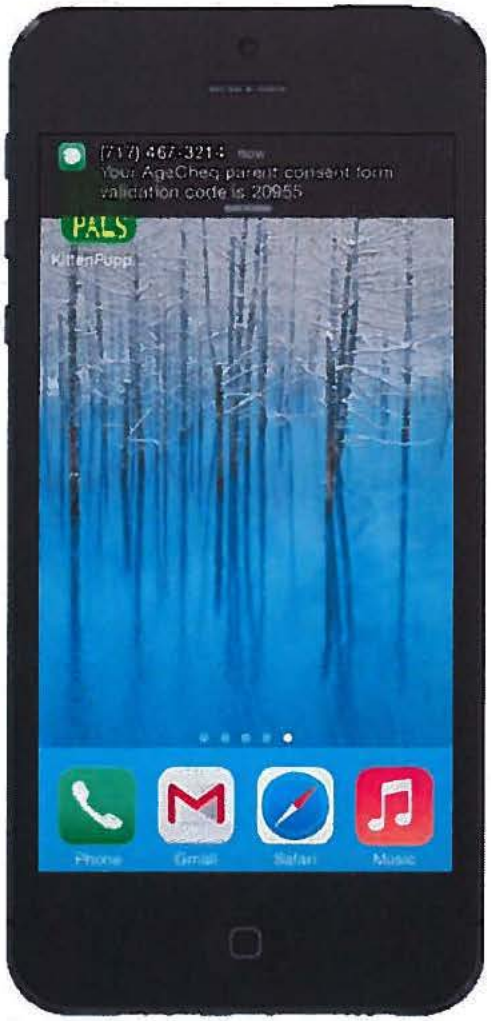
address line 2

Anytown MD 12345

Your Birth Year: 1970

Mobile Phone Number: 555 555 1212

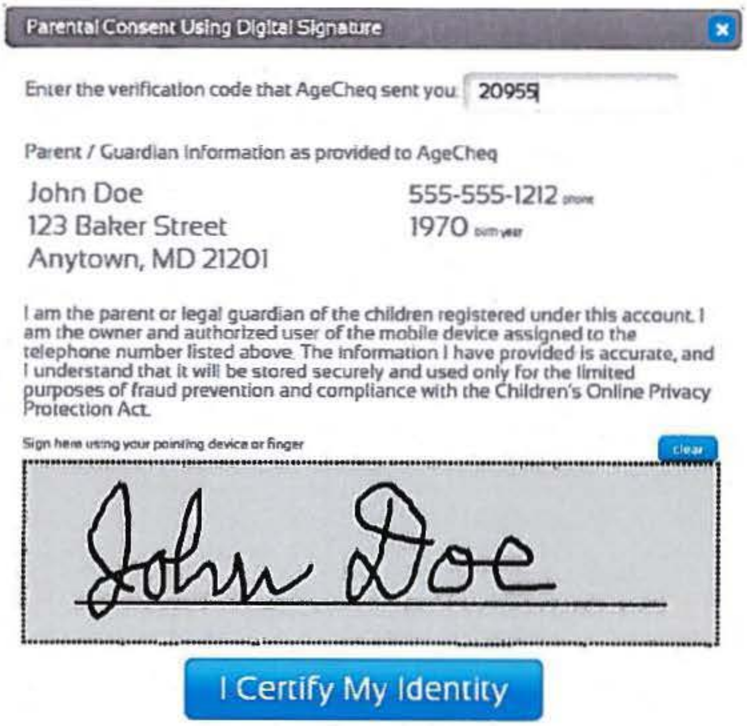
Figure 2- Parental Information Capture Screen



(717) 467-3214 now

Your AgeCheq parent consent form validation code is 20955

Figure 3- Parent's Mobile Device Receives Verification Code By Text Message



Enter the verification code that AgeCheq sent you: 20955

Parent / Guardian Information as provided to AgeCheq

John Doe
123 Baker Street
Anytown, MD 21201

555-555-1212 phone
1970 birth year

I am the parent or legal guardian of the children registered under this account. I am the owner and authorized user of the mobile device assigned to the telephone number listed above. The information I have provided is accurate, and I understand that it will be stored securely and used only for the limited purposes of fraud prevention and compliance with the Children's Online Privacy Protection Act.

Sign here using your pointing device or finger

John Doe

Figure 4-Verification Code Entry and Signature Capture Screen