Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)	
	)	
AgeCheq Application for Parental Consent Method	)	P–155400
	)	

COMMENTS OF CENTER FOR DIGITAL DEMOCRACY

The Center for Digital Democracy ("CDD") respectfully submits these comments in response to the *AgeCheq Application for Parental Consent Method, Project No. P–155400,* filed with the Federal Trade Commission.[1] CDD is a national nonprofit, nonpartisan organization dedicated to promoting responsible use of new digital communications technologies, especially on behalf of children and their families. CDD has a strong interest in ensuring that the Commission only approves verifiable parental consent ("VPC") methods that fully comply with FTC's rules and with the underlying purpose of the Children's Online Privacy Protection Act ("COPPA"). As detailed in these comments, AgeCheq's application for approval of its VPC mechanism fails to meet the requirements set forth in the COPPA Rule and should be denied.

I. AgeCheq's Application

AgeCheq's proposed verifiable parental consent mechanism involves essentially three steps, which an intermediary (such as AgeCheq) facilitates through a portal.[2] First, the parent visits the intermediary and signs up for the service by submitting certain personal information, "minimally name, address, birth year, and mobile telephone number," to the intermediary.[3] Second, the intermediary sends a confirmation code to that mobile phone number via text message, which the parent then uses to verify his or her identity to the intermediary through the

[1] 79 Fed. Reg. 70135 (Nov. 25, 2013).
[2] This application is submitted independently of AgeCheq's first application submitted on July 25, 2014. Appl. at 2 n.3. Thus, it must stand on its own.
[3] Appl. at 3.

portal. Third, the parent signs a "statement of certification" verifying ownership of the device and the accuracy of the information he or she previously submitted. Once signed, the verification is then permanently tied to the mobile device used. Operators that use the intermediary can rely on the verification when attempting to solicit parental consent for their services. The proposed system stores the information securely, but can be decrypted if "there is a need to review" it.[4]

II. The FTC should reject AgeCheq's proposal.

AgeCheq's application is deficient in at least two ways. First, it is not reasonably calculated to ensure the person granting consent is the child's parent. Second, it poses significant risks to consumers' personal information.

A. Response to Question 2: The proposed VPC mechanism is not reasonably calculated to ensure the person granting consent is the child's parent.

AgeCheq's proposal does not meet the "reasonably calculated" requirement because it makes no effort to ensure that the person granting consent is the child's *parent*. AgeCheq acknowledges the potential for "child bad actor[s]" but its proposal does not protect against them. In fact, there are numerous ways the proposed system would be easily fooled into verifying many non-parents. For example, a child could easily make up a name, address, and birth year, or use the information of a sibling, other family member, or essentially anyone. This system has no way to ensure the accuracy of the information submitted. It simply takes the information as a given. So long as the mobile phone number is a real phone number capable of text messaging (it could even be the child's phone number), the system will verify the "parent."

The proposed mechanism does not collect information or ask questions that only a parent would know. Children are very likely to know their parent's name, address, and birth year. Prior VPC mechanisms were approved by the FTC because the information collected was out-of-

[4] Appl. at 4.

wallet and difficult for a child to know (so-called "knowledge-based authentication" or "KBA").[5] This proposal has none of the indices of accuracy that KBA has, even though CDD maintains that KBA is still insufficient in the children's privacy area where the goal is to ensure the person granting consent is the child's parent.

Also, the method has no means of verifying that the signature actually belongs to the parent. The FTC recognized this issue in their Statement of Basis and Purpose when it declined to allow simple digital signatures to indicate parental consent.[6] In the scenario described above where a child inputs the request information, the child could easily sign the verification, and AgeCheq would have no way to know that it was the child's signature. Thus, this proposal fails to provide further indicia of reliability to the digital signature.

The application does not provide marketplace evidence or research that shows the system would ensure parents are the ones providing consent. The FTC rejected AssertID's proposal in part for this reason.[7] AgeCheq does draw a parallel to the apps WhatsApp and Pango, which also rely on a registration and validation code process. Those apps, Pango being a parking app, are not intended for children. Therefore, whether the process works for those apps is inconsequential to the application at issue, which must meet the requirements of the COPPA Rule.

Last, AgeCheq argues that this system is "harder to evade than the 'sign and send' paper form method."[8] This is not true. Physically filling out a form with information, signing it, obtaining an envelope and stamp, addressing the envelope, and taking the envelope to the

[5] Letter from April J. Tabor, Acting Secretary, FTC, to Marshall C. Harrison, CEO, Imperium, LLC, Dec. 23, 2013, http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf.
[6] Statement of Basis and Purpose, 78 Fed. Reg. 3972, 3988 (Jan. 17, 2013) ("SBP").
[7] Letter from Donald S. Clark, Secretary, FTC, to Keith Dennis, President, AssertID, Inc., Nov. 12, 2013, http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-denies-assertids-application-proposed-coppa-verifiable-parental-consent-method/131113assertid.pdf.
[8] Appl. at 7.

mailbox (or a post office) is actually much more involved than the process AgeCheq has proposed. And a mailed envelope is stamped with the zip code of the sender, which increases the indicia of reliability. In other words, the sign and send method is reliable because it involves many physical steps that a child is unlikely to accomplish on his or her own. The AgeCheq proposal has actually removed many of these additional steps and replaced them with easily-accomplished steps that require only a phone number. In fact, one of the selling points of the system is that it "allows parents to conveniently provide verifiable consent."[9] AgeCheq's proposal is all digital and requires almost no writing. Digital signatures are easily forged and are often illegible, which does not increase the reliability of the mechanism.[10]

B. Response to Question 3: The proposal poses significant risk to consumers' information.

The proposed method poses a clear risk to consumers and their personal information. AgeCheq's proposal collects information from parents and then the operator or intermediary "Securely Stores Parent Name, Address, Birth Year, Phone Number, Image of Signature."[11] This information can then be "retrieved, decrypted . . . and reviewed."[12] AgeCheq even admits that "all methods necessarily involve the collecting and/or storing of personally identifiable parental information," but AgeCheq inappropriately downplays the risks inherent in its mechanism.[13]

---

[9] Appl. at 9 (emphasis added).

[10] The FTC should seek more information from AgeCheq when it claims that "[c]hildren are less likely to encounter the form." Appl. at 6. In order for the VPC mechanism to work, it would have to inform the child, prior to use of the app, that he or she cannot play the game or view the content without a parent's permission. Then, the app would have to show the child how the parent can give their permission, which would create the opportunity for the child to "encounter" the form.

[11] Appl. at 5.

[12] *Id.* at 4.

[13] *Id.* at 8-9.

AgeCheq's proposal contemplates that intermediaries or operators will store parental information indefinitely. AgeCheq does not indicate for what purpose that data will be stored.[14] AgeCheq makes no provision for parents to delete the information if necessary. While AgeCheq claims that the data can be reviewed, it does not explain how a parent might do so and what hoops it will require parents to jump through before they can review the information on file. Will the data be easily retrievable on the phone? Will a special request be required? Will the parent have to call AgeCheq? What happens if the parent upgrades his or her phone? What happens when the child turns 13 years old? None of these basic questions are answered in this application.[15] Parents would want to know this information before handing over personal data so their children can play a game.

If the FTC were to approve this proposed method, it should make clear that data collected by the intermediaries must be encrypted in transit and at rest and should impose heightened password requirements that would improve the security of the stored information. AgeCheq claims "the privacy practices of the intermediary [using this proposal] are . . . germane,"[16] and that AgeCheq itself encrypts and stores data "in secure cloud storage using AES 256 encryption and dual key HMAC authentication."[17] While AgeCheq's use of AES 256 encryption and dual key HMAC authentication is promising, the FTC should require this encryption (or better) if other providers want to claim to use an "FTC-approved" VPC mechanism.

---

[14] AgeCheq does claim, in a footnote, that "[s]ecurity is a concern" and that "identifiable information . . . is never shared, and used only for purposes of delivering AgeCheq's COPPA consent and related services." Appl. at 4 n.7. This begs the question of why AgeCheq retains the parent's information indefinitely.

[15] AgeCheq's lack of explanation of its mechanism also violates the requirement that "applicants . . . [are] required to present a detailed description of the proposed mechanism." SBP, 78 Fed. Reg. at 3991.

[16] Appl. at 4, n.7.

[17] *Id.*

Conclusion

This mechanism cannot be approved because it is unreliable, easily circumvented by children, and poses significant risk to consumer information.

Respectfully submitted,

/s/

Eric G. Null
Angela J. Campbell
Institute for Public Representation
Georgetown Law Center
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9535

Counsel for Center for Digital Democracy

Dated: December 29, 2014