

*Before the*  
FEDERAL TRADE COMMISSION  
Washington, DC 20580

<b>In the Matter of</b>	)	
	)	
<b>AgeCheq Application for Parental</b>	)	
<b>Consent Method</b>	)	<b>Project No. P-145410</b>

**COMMENTS OF CENTER FOR DIGITAL DEMOCRACY & CAMPAIGN FOR A  
COMMERCIAL-FREE CHILDHOOD**

The Center for Digital Democracy (CDD) and Campaign for a Commercial-Free Childhood (CCFC) (collectively, Commenters) respectfully submit these comments in response to the Federal Trade Commission’s (FTC or the Commission) *Children’s Online Privacy Protection Rule: AgeCheq Application for Parental Consent Method*.<sup>1</sup> 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. CCFC is a national coalition that counters the harmful effects of marketing to children. Commenters have a strong interest in ensuring that FTC only approves self-regulatory structures that fully comply with the agency’s rules and with the underlying purpose of the Children’s Online Privacy Protection Act (COPPA), *i.e.* to prohibit the collection of personal information from children without the verifiable informed consent of their parents.

---

<sup>1</sup> 79 Fed. Reg. 51514 (Aug. 29, 2014) [hereinafter VPC Notice].

## INTRODUCTION

AgeCheq submitted an application to FTC on July 25, 2014, that is “REDACTED FOR PUBLIC INSPECTION”<sup>2</sup> and in doing so invited the public to comment on its proposal and investigate its business practices to see if they are effective. There is nothing in this application that would constitute a “detailed description,” which is the standard that must be met before FTC initiates this type of review. This submission, ostensibly an application for a new Verifiable Parental Consent (VPC) method under COPPA, reveals that AgeCheq is not proposing a new VPC method. Additionally, the company’s submission and its website illustrates that it is deceiving its customers, treating parents unfairly, violating COPPA, allowing children to impersonate their parents and approve all future information collection by any app, and is unnecessarily collecting sensitive personal information from parents outside its COPPA duty to verify their identities. Commenters request that FTC disregard this application as not sufficient for a VPC method proposal. Moreover, Commenters request FTC commence investigating AgeCheq for multiple unfair and deceptive offenses, evident in this application and on the company’s website, against consumers and app developers.

## ANALYSIS

### **I. AgeCheq’s Application Proposes no new VPC Method and Even if it did it Lacks a Detailed Description of its System or any Sort of Evidence that it is Effective**

Like the iVeriFly VPC application on which FTC took no action earlier this year, this application is mooted by the fact that it proposes no new VPC method for verifying parental

---

<sup>2</sup> 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), [hereinafter App.] *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>.

identity. Even under a tortured understanding of “verifiable parental consent” that extends to whatever AgeCheq might be proposing, this application was deficient from inception because it lacks basic showings (detail and evidence of effectiveness) that are required under the voluntary approval portion of COPPA.

**a. The application uses only enumerated VPC methods and therefore is an inappropriate submission, deserving of no response**

As the FTC’s VPC Notice says, a central question of approving any new method of obtaining VPC is whether it is in fact new: “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) [sic] of the Rule?”<sup>3</sup> Existing VPC methods are listed in § 312.5(b)(2) of the COPPA Rule,<sup>4</sup> and also include knowledge-based authentication, approved by the Commission in December 2013.<sup>5</sup> AgeCheq’s proposal states it will only use existing VPC methods and therefore is not deserving of FTC review or approval.

All accepted forms of VPC verify, at the outset, that a new user is actually an adult who is likely to be the parent of an identified child. *See* § 312.5(b)(2) and knowledge-based authentication.<sup>6</sup> This is an important step in COPPA and the proper implementation of VPC has been hotly contested by commenters over the years.<sup>7</sup> It is distinct from re-identification of a

---

<sup>3</sup> VPC Notice, *supra* note 1, at 51515.

<sup>4</sup> 78 Fed. Reg. 3972, 4011 (Jan. 17, 2013).

<sup>5</sup> Press Release, FTC, FTC Grants Approval for New COPPA Verifiable Parental Consent Method (Dec. 23, 2013), *available at* <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>.

<sup>6</sup> Press Release, FTC, FTC Grants Approval for New COPPA Verifiable Parental Consent Method (Dec. 23, 2013), *available at* <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>.

<sup>7</sup> *See* 78 Fed. Reg. 3972 (Jan. 17, 2013) (discussing many commenters’ submissions on VPC methods); 64 Fed. Reg. 59888 (Nov. 3, 1999) (same).

known user, which almost all online services now effectuate with passwords and similar technologies (i.e. two-step verification), because VPC is the gate through which all re-identified users must first pass. VPC is an identity control that sets a user apart from the entire online population, re-identification of an existing user is merely the recognition that this individual has already passed the VPC test. However, AgeCheq’s application focuses on the novelty of its device-based re-identification and calls this VPC,<sup>8</sup> in a misunderstanding of this central tenant of COPPA.

In February of this year FTC concluded a review of iVeriFly’s proposed new VPC method.<sup>9</sup> iVeriFly had proposed to combine an already-approved method of verification, Social Security Number verification, with another VPC method that had been approved while iVeriFly’s application was pending, knowledge-based authentication.<sup>10</sup> Since the application only considered two existing VPC methods, FTC “determined it was unnecessary to approve the company’s specific method” and sent the company a letter closing agency review.<sup>11</sup> The Commission had opened the comment period<sup>12</sup> when one of the proposed VPC methods was yet to be approved, but as soon as it was evident that the application was redundant FTC ended its review.

---

<sup>8</sup> See generally App., *supra* note 2.

<sup>9</sup> Press Release, FTC, FTC Concludes Review of iVeriFly’s Proposed COPPA Verifiable Parental Consent Method (Feb. 25, 2014), *available at* <http://www.ftc.gov/news-events/press-releases/2014/02/ftc-concludes-review-iveriflys-proposed-coppa-verifiable-parental>.

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*; see also Secretary Donald S. Clark letter, iVeriFly, Inc.’s Application for Approval as a COPPA Verifiable Consent Mechanism (FTC Matter No. P135420), (Feb. 24, 2014), *available at* <http://www.ftc.gov/system/files/attachments/press-releases/ftc-concludes-review-iveriflys-proposed-coppa-verifiable-parental-consent-method/140225iveriflyapplicationletter.pdf>.

<sup>12</sup> Press Release, FTC, FTC Seeks Public Comment on iVeriFly, Inc., Proposal for Parental Verification Method Under COPPA Rule (Dec. 16, 2013), *available at* <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-public-comment-iverifly-inc-proposal-parental>.

It is clear from AgeCheq’s application that it is not proposing any new VPC methods, and therefore FTC review, including this comment period, is a waste of agency resources. “The proposed method incorporates . . . tried and true (legacy) methods to verify parental identity . . . .”<sup>13</sup> The application says that AgeCheq is only proposing to “verif[y] parental identity through any currently enumerated method” from 16 CFR § 312.5(b)(2).<sup>14</sup> It is revealed later in the application that AgeCheq is even more selective than that, using only two methods—financial transactions and/or print-and-send parental verification, both enumerated in the current COPPA Rule<sup>15</sup> and dating back to the beginning of COPPA.<sup>16</sup> The video AgeCheq provides as a citation, discussed more fully below, reiterates this, saying: “There are two methods to verify that the current user is an adult. The user may either execute a credit card transaction, or they may sign and return an identity declaration form. *Both of these methods are enumerated in the rule.*”<sup>17</sup> (emphasis added). There is no new proposed VPC method in the company’s application, and therefore it does not merit this proceeding.

**b. Even assuming this application presents a new method, it is deficient and should not have been approved for notice and comment rulemaking**

*i. The application is deficient on its face*

Even if this was somehow deemed a new VPC method this application falls far short of the requirements for a filing under § 312.12(a). This relates to FTC’s second question:

---

<sup>13</sup> App., *supra* note 2, at 1–2.

<sup>14</sup> *Id.* at 2.

<sup>15</sup> 78 Fed. Reg. 3972, 4011 (Jan. 17, 2013) (listing these methods under §§ 312.5(b)(2)(i)–(ii)).

<sup>16</sup> See 64 Fed. Reg. 59888, 59914 (Nov. 3, 1999) (in the first iteration of the COPPA Rule both print-and-send and credit card transactions were on the list of approved methods in § 312.5(b)(2)).

<sup>17</sup> Vimeo, Real-Time Common Consent Mechanism Preferred User Flow: Parent Sets Up Account First, <http://vimeo.com/agecheq/review/101104468/7e7ae4941c> (last visited Sept. 16, 2014).

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.<sup>18</sup>

The requirements AgeCheq must meet include the basic hurdle: “To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with analysis of how the methods meet § 312.5(b)(1).” § 312.12(a).<sup>19</sup> FTC's consideration of this application ignores the fact that there is nothing in the public record that satisfies either the “detailed description” or “analysis of how the methods meet § 312.5(b)(1).” Without even a small showing of either of these requirements this public review is improper under § 312.12(a).

This is a vague application, full of extraneous content that is not responsive to the above requirements. AgeCheq's application is seventeen pages long<sup>20</sup>—and only that many if one counts the vague charts,<sup>21</sup> redacted empty space,<sup>22</sup> and superfluous footnotes.<sup>23</sup> Of that, two pages are an introductory summary,<sup>24</sup> eight pages are AgeCheq's (heavily editorialized)<sup>25</sup> opus

---

<sup>18</sup> VPC Notice, *supra* note 1, at 51515.

<sup>19</sup> *See also* similar language in *id.* at 51514.

<sup>20</sup> *See* App., *supra* note 2.

<sup>21</sup> *Id.* at 10, 14–16.

<sup>22</sup> *Id.* at 11.

<sup>23</sup> *See, e.g., id.* at 3 n.7 (citing to the entire Wikipedia page for the iPhone for the fact that iPhones are newer than COPPA); *id.* at 9 n.28 (stating that FTC's statement of basis and purpose “mistakenly refers at page 3,990 [sic] to ‘Section 312.5(3)’ . . .” and then provides a detailed discussion of AgeCheq's legal assumptions that brought it to § 312.12 in a paragraph that is significantly more specific than any discussion provided on how the company's technology is meant to work).

<sup>24</sup> *Id.* at 1–2.

<sup>25</sup> *See, e.g., id.* at 8 (“For the Commission, charged by law with enforcing COPPA, this ‘scofflaw’ climate is frustrating, but hard to counteract with limited enforcement resources.”).

on the history of COPPA,<sup>26</sup> less than six pages purport to describe the “verification method,”<sup>27</sup> approximately four pages are taken up with basic flowcharts that simplify and restate the information in the rest of the application,<sup>28</sup> and at the end, a page and a half summary conclusion.<sup>29</sup> Nowhere in this document does the company offer technical specifications of how it purports to do any of the things it claims to do, nor does it rely on studies or industry practice to validate its proposal.<sup>30</sup> This proposal is for a technological implementation of VPC that never gives a description of the technology, for example saying it will use “unique identifiers” and “validation checking code” generally but never naming what persistent identifiers will be used or anything further about the code.<sup>31</sup> Nowhere in this document does it describe what parents will

---

<sup>26</sup> *Id.* at 2–9.

<sup>27</sup> *Id.* at 9–14. This section contains a half page of “REDACTED” information and an illustrative flowchart that does not detail how the proposed method works.

<sup>28</sup> *Id.* at 10, 14–16. The final half page of the description of the company’s “verification method” is entirely taken up by a summary of the topics covered by the figures that summarize how the proposed method should work, so the above page counts should be viewed as over-inclusive since the company has gone to great lengths to summarize what its summaries of its summary of its proposed method will entail. *See id.* at 14.

<sup>29</sup> *Id.* at 16–17.

<sup>30</sup> *Compare App. with AssertID*, Request for review and approval of AssertID’s “verifiable parental consent” method under Part 312.12(a) of the Children’s Online Privacy Protection Rule., June 28, 2013, <http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-seeks-public-comment-assertid-inc.proposal-parental-verification-method-under-coppa-rule/130815assertidapplication.pdf> (relying on sociological studies and a patent application containing technical descriptions of the proposed method and the science upon which it is based); *Imperium*, Second Revised 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), Aug. 12, 2013, <http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-seeks-public-comment-imperium-llc-proposal-parental-verification-method-under-coppa-rule/130909imperiumapplication.pdf> (relying on industry practice in other online verification situations).

<sup>31</sup> *App.*, *supra* note 2, at 11, 12.

be asked to give up in order to take advantage of its online portal, though this information is incompletely disclosed in online videos AgeCheq cites to.

This application is an exercise in how insufficient an application can be and still garner FTC review. Other VPC submissions FTC has considered have relied on evidence in the form of industry practice and scientific studies, and such information was available even in redacted applications made available for public comment.<sup>32</sup> This application either never had such information, or it has been redacted so heavily that all that is left is AgeCheq's assertions that the company invented something amazing ("Importantly, the proposed method is not only feasible—it is available today.").<sup>33</sup> Whatever the company is proposing remains totally opaque to the public.

*ii. The videos AgeCheq cites to show practices that undercut COPPA, and do not demonstrate or prove the effectiveness of a VPC method in any way*

The company's citation to its three online videos does nothing to cure the insufficiency of its written application. As an initial matter, the citations only state "For a video demonstration of this process, please visit . . ." <sup>34</sup> so they do not inform FTC or the public that there is any information available to supplement the descriptions contained in the company's basic flow charts. The videos are short (approximately three to six minutes in length) walk-throughs of how some parts of AgeCheq's platform might look to a parent who is registering for the company's service.

---

<sup>32</sup> See *supra* note 30.

<sup>33</sup> App., *supra* note 2, at 14. From a legal standpoint the current availability of an ineffective branded product is not important to FTC's approval of that product as a VPC method.

<sup>34</sup> See *id.* at 14 n.32, 15 n.35, & 16 n.34.

The first<sup>35</sup> shows that parents will be required to provide their own street address and partial Social Security Number in order to gain access to AgeCheq’s portal. These requirements are not part of either of AgeCheq’s chosen VPC methods (i.e. credit card and print-and-send verification do not require the storage of that information long-term), and therefore seem to be additional collection of personal information from parents that the company does not need for COPPA purposes, and evidently retains long-term with a parent’s account. In response to FTC’s question 3 in its VPC Notice, this will “pose a risk to consumers’ personal information” and such risk is not “outweighed by the benefit to consumers and businesses”<sup>36</sup> as it is of no apparent value to parents and can only serve AgeCheq as a horde of personal information it might lose in a data breach, or sell to other entities.

The second,<sup>37</sup> and longest, video shows a disclosure to parents including the fact that the demonstration app “stores” a child’s Facebook information. It is not explained in this video what “stores” means in this case, but since Facebook is an online service forbidden to users under thirteen<sup>38</sup> it raises questions that AgeCheq is planning to collect and use such information obtained from children (and apparently will allow some apps to “share” the information with third parties, see screen shot below). Additional parts of the “just-in-time” disclosure shown in the video are confusing even to one who is familiar with the requirements of COPPA disclosures

---

<sup>35</sup> Vimeo, Real-Time Common Consent Mechanism Preferred User Flow: Parent Sets Up Account First, <http://vimeo.com/agecheq/review/101104468/7e7ae4941c> (last visited Sept. 16, 2014).

<sup>36</sup> VPC Notice, *supra* note 1, at 51515.

<sup>37</sup> Vimeo, Real-Time Common Consent Mechanism Likely User Flow: Child Finds App First, <http://vimeo.com/agecheq/review/101104516/935919e707> (last visited Sept. 19, 2014).

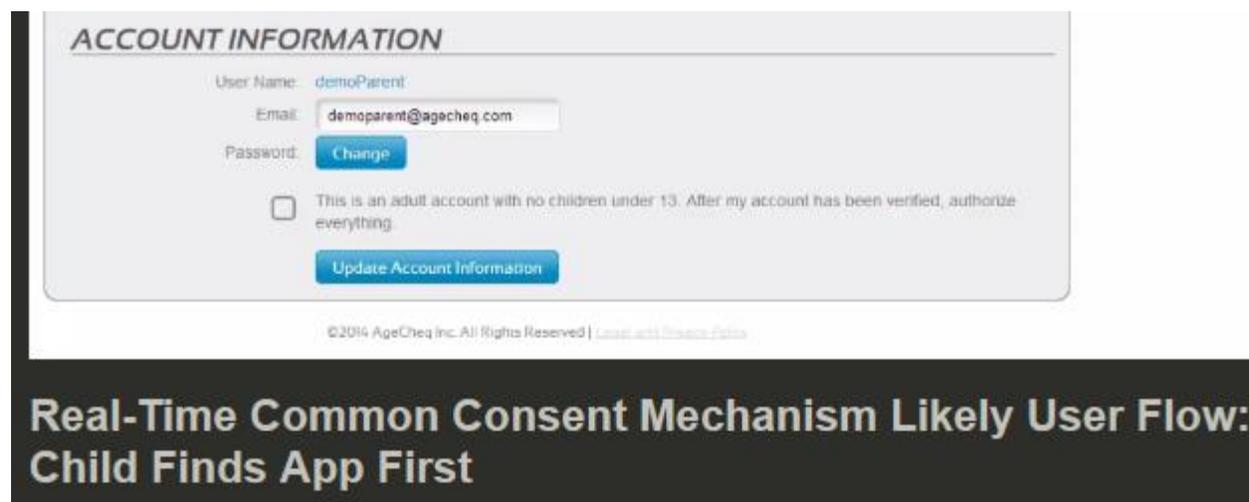
<sup>38</sup> Facebook, Statement of Rights and Responsibilities, Nov 15, 2013, <https://www.facebook.com/legal/terms> (“Here are some commitments you make to us relating to registering and maintaining the security of your account: . . . You will not use Facebook if you are under 13.”).

and what information is normally included therein: e.g. there is no explanation of the difference or significance between AgeCheq’s use of “collected” and “stored” for children’s IP addresses:



This video also shows that AgeCheq includes a single check box that would allow parents (or children who have access to a parent device, discussed *infra*) to *approve all current and future collection on all apps that have self-identified as child-directed* using AgeCheq’s service. The

option reads: “This is an adult account with no children under 13. After my account has been verified, authorize everything.”



This is disconcerting both from the standpoint that this encourages parents to take advantage of a large new exception to COPPA for *child-directed* apps (nowhere suggested in the COPPA Rule), and from the standpoint that any child who temporarily gains access to their parent’s AgeCheq account can, with a single click, provide themselves with seamless approval for all current and future app data collection. This is a major design flaw that poses a significant risk to child privacy.

The third video further emphasizes that parental consent “can be given in under a minute.”<sup>39</sup> While this is exemplary efficiency, COPPA does not require VPC methods to be efficient—it requires them to be effective. *See* § 312.5. The application says that parents will receive “layered” COPPA disclosures and that the portal “offers parents many different ways” to view disclosures,<sup>40</sup> but in these videos these options and layers obfuscate any meaningful

<sup>39</sup> Vimeo, Real-Time Common Consent Mechanism User Flow For Typical Use After Initial Setup, <http://vimeo.com/agecheq/review/101104651/44bb720002> (last visited Sept. 16, 2014).

<sup>40</sup> App., *supra* note 2, at 12, 13.

disclosure of data practices. As noted in the last paragraph, the short and confusing one-word disclosures that AgeCheq uses might be easy to glance over but they do not tell parents how information is being collected, used, and shared. Moreover, as can be seen in this third video, at the bottom of this disclosure the company provides a large green “I approve” button and two significantly smaller buttons, in the same color as the dark background, for “view full policy” and “approve with no sharing.”<sup>41</sup>



Not only does this discourage the parent from pursuing either of these options, which are both mandated by COPPA, but it also does not include an “I do not approve” button, seemingly forcing a parent to choose from different ways of opening their child to privacy invasion one way or another.<sup>42</sup> Commenters agree with AgeCheq that this is a highly efficient way to get someone to click on an approval button, but that consent is legally invalid when done without proper disclosures or under the duress of unfair options that do not abide by COPPA.

While these three videos do nothing to satisfy AgeCheq’s duty to provide a detailed description of its proposed method, or how it satisfies § 312.5(b)(1)’s proof standard, they do show that the company has failed to make a COPPA-compliant system that will inform parents of company practices or keep children from divulging personal information without the real informed consent of their parents. As will be seen in the next section this is especially

---

<sup>41</sup> Of course approving an app with no sharing does nothing to limit the app’s collection and use of children’s personal information, so this last option is not the same as a disapproval.

<sup>42</sup> *Id.*

concerning due to the information that AgeCheq did not include in its application, but which it makes available to any app developers that it views as potential clients.

**II. AgeCheq’s Application Makes Clear that it is Violating Both Section 5 of the FTC Act by Deceiving Potential Clients and Using an Unfair Identification System, as well as Violating COPPA in its Role as an Operator Tracking Children**

By initiating this review AgeCheq has asked FTC and the public to vet its practices to see if they comply with one small portion of COPPA, but once this scrutiny is invited Commenters and the Commission cannot ignore obvious violations of the law. This application and the company’s website reveal that it is a willful violator of both the FTC Act and COPPA. AgeCheq’s Section 5 violations make COPPA violators out of all of its customers, multiplying the damage done to the industry and child privacy. Such a submission calls for FTC to investigate and seek injunctions against AgeCheq, not support its business model by indulging this proposal.

**a. AgeCheq’s representations to its potential clients show this application under § 312.12(a) is misfiled and the company should either submit an application to become a COPPA Safe Harbor and otherwise cease deceiving app developers about its business**

There are three parts to a deception under the FTC Act. First, there must be a representation, omission, or practice that is likely to mislead the consumer. Second, the act or practice must be evaluated from the perspective of a reasonable consumer. Third, the representation, omission, or practice must be material. In this case the reasonable consumer is a programmer with no significant knowledge of COPPA’s requirements. This is because AgeCheq is targeting app developers who are “small businesses and even individuals”<sup>43</sup> and these “small

---

<sup>43</sup> App., *supra* note 2, at 5.

developers with few resources for the costly and complicated parental verification and consent process”<sup>44</sup> are more easily deceived than established companies that have resources to do research that would reveal AgeCheq’s misrepresentations of fact and law.

It can be seen from AgeCheq’s marketing materials aimed at app developers that it makes itself out to be a COPPA Safe Harbor, and therefore should be investigated by FTC for deceptive practices unless it files a full Safe Harbor application under § 312.11.

AgeCheq’s application alludes to this deception<sup>45</sup> but it is more apparent when one looks at its materials for prospective clients. When a developer first visits the company’s site, AgeCheq presents itself as an expert in COPPA compliance that will shield cooperating developers from FTC oversight and fines. On several pages, including its home page, it refers to itself as a “COPPA Compliance Ecosystem,”<sup>46</sup> which implies that it provides the full suite of tools necessary to comply with all of COPPA.<sup>47</sup> Its home page has a link to a quiz under the prompt “Is Your Game at Risk for a Big COPPA Fine?” and claims that AgeCheq is all that is needed for a Developer to comply with COPPA.<sup>48</sup>

---

<sup>44</sup> *Id.* at 16.

<sup>45</sup> On page one of the application AgeCheq tells FTC that its platform will “facilitate the entire range [of] requirements under the Children’s Online Privacy Protection Act” despite the fact that the company is applying to be a VPC and not a full COPPA Safe Harbor. *Id.* at 1.

<sup>46</sup> AgeCheq <http://www.agecheq.com/> (last visited Sept. 16, 2014) (the home page goes on to say that “We make it easy for developers to comply with COPPA law, and for parents to regain control of their children’s online privacy.” further brining home this point).

<sup>47</sup> Compare this usage with App., *supra* note 2, at 5, 16 (using the word “ecosystem” to describe the entire mobile app market).

<sup>48</sup> AgeCheq <http://www.agecheq.com/> (last visited Sept. 16, 2014).



Is Your Game At Risk for a Big COPPA Fine?

Take our short four question survey to find out.

← [TAKE THE SURVEY NOW](#) →



Is Your Game At Risk for a COPPA Fine?

WHAT IS AGECHEQ? DEVELOPERS SERVICE PROVIDERS PARENTS

## COPPA Compliance is Easy for Developers.

Comply with COPPA requirements quickly while giving parents a dramatically better experience.

← **It's free for developers.**

[LEARN MORE ABOUT PROTECTING YOUR BUSINESS](#) →



APP/DEVICE	ACCOUNT	REPORTS
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7
8	8	8
9	9	9
10	10	10

On AgeCheq’s site for app developers it claims to be “[t]he free, painless way for developers to comply with COPPA.”<sup>49</sup> The same page tells developers that using AgeCheq will help them to avoid FTC oversight and fines<sup>50</sup>—traditionally the domain of COPPA Safe Harbors. *See* § 312.11(g) (“An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8 and 312.10 if that operator complies with Commission-approved safe harbor program guidelines.”). However, AgeCheq is not an approved COPPA Safe Harbor<sup>51</sup> and has not sought to become one.<sup>52</sup>

In light of recent FTC enforcement under COPPA, AgeCheq has used the Commission’s press to further expand its user base with statements that it can stop agency oversight. Last week it issued a press release stating, “The AgeCheq compliance cloud service was designed to scale to support real-time COPPA compliance for the entire mobile game industry.”<sup>53</sup> Following FTC actions against Yelp and Tiny Co., “AgeCheq has seen an immediate spike in interest in compliance from those with the biggest risk: top-tier publishers with hundreds of millions of installed users.”<sup>54</sup> The release goes on to make promises to get clients in compliance with all of COPPA:

---

<sup>49</sup> AgeCheq for App Developers [http://www.agecheq.com/?page\\_id=7](http://www.agecheq.com/?page_id=7) (last visited Sept. 16, 2014).

<sup>50</sup> *Id.* (“We’re betting you’ll quickly add all of your apps and eliminate the risk of a huge FTC fine for COPPA non-compliance.”)

<sup>51</sup> FTC, Safe Harbor Program <http://www.business.ftc.gov/content/safe-harbor-program> (last visited Sept. 16, 2014) (listing all approved COPPA Safe Harbors).

<sup>52</sup> While it is possible that AgeCheq has a pending confidential application with FTC to become a Safe Harbor, the instant application to become a VPC common consent mechanism seems to rule out that possibility.

<sup>53</sup> Press Release, AgeCheq supports over 400 million app starts per day as FTC COPPA enforcement leaves game publishers scrambling to comply with 2012 law (Sept. 24, 2014), *available at* <http://www.mobilitywire.com/agecheq/2014/09/24/8498>.

<sup>54</sup> *Id.*

With AgeCheq, publishers can easily comply with COPPA by creating a developer account, then adding a few lines of code to each of their games using the company's native SDKs for iOS, Android, Unity, Corona or HTML5. . . . App and game publishers of any size *wishing to avoid legal fees, fines, and annual privacy audits that face COPPA violators* can learn more about AgeCheq's COPPA compliance cloud service at [www.AgeCheq.com](http://www.AgeCheq.com).<sup>55</sup>

(emphasis added). But as is explained above, going to the company's website will only lead potential clients to believe AgeCheq is a Safe Harbor that will fully protect them from FTC enforcement. The fact that the company is now expanding its service to "top-tier publishers with hundreds of millions of installed users" in the children's market is cause for immediate FTC investigation.

The videos that AgeCheq did not include in its current application to FTC further reinforce its message to developers that it is essentially a Safe Harbor. On the developer page, discussed above, there is a video that mischaracterizes COPPA as only three things, i.e.: VPC; just-in-time disclosure; and managing parental contact.<sup>56</sup> While it is true that these are some of COPPA's requirements, they are hardly all an app developer must do to comply with the law. The video goes on to say that a developer need only insert AgeCheq's code into their existing app and they will be COPPA compliant "in a single day."<sup>57</sup> In another video for developers titled "What is AgeCheq?" the company reiterates that AgeCheq is supplying a "painless" COPPA compliance "ecosystem."<sup>58</sup> The following images represent some of these statements by the company in the marketing videos:

---

<sup>55</sup> *Id.*

<sup>56</sup> Vimeo, AgeCheq For App Developers, <http://vimeo.com/79986206> (last visited Sept. 16, 2014).

<sup>57</sup> *Id.*

<sup>58</sup> Vimeo, What is AgeCheq? <http://vimeo.com/77859701> (last visited Sept. 16, 2014).

**INTEGRATING AGE CHEQ**

SDKS FOR IOS, ANDROID, HTML5

**FREE**

**MAKE YOUR APPS COPPA COMPLIANT IN 1 DAY**

**AgeCheq For App Developers**

from **AgeCheq** **PRO** 9 months ago NOT YET RATED

**AgeCheq**

**CREATE YOUR DEVELOPER ACCOUNT TODAY**

**BE COPPA COMPLIANT TOMORROW!**

**AgeCheq For App Developers**

from **AgeCheq** **PRO** 9 months ago NOT YET RATED

What is misleading about these statements is that COPPA contains other compliance duties beyond the three listed, and there is no quick fix for a poorly designed app that did not comply with COPPA the previous day. As one example, the COPPA Rule requires “reasonable procedures to protect the confidentiality, security, and integrity of personal information collected

from children.” § 312.8. But the vast majority of apps are currently not living up to this basic standard of data security. Recent studies show that many of the most popular Android apps are not secured and retain, and make available unencrypted, private communications and other content (i.e. location and photographs) for weeks after information is sent.<sup>59</sup> Additionally, COPPA requires app developer operators to provide full, meaningful, and non-confusing disclosures of their privacy practices regarding children. § 312.4(d). In 2012 FTC found that children’s apps fail to properly disclose privacy practices in a single understandable policy,<sup>60</sup> and a recent global study shows that 85 percent of all apps have no basic privacy disclosure.<sup>61</sup> The “survey of over 1,200 mobile apps by 26 privacy regulators from across the world has shown that a high number of apps are accessing large amounts of personal information without adequately explaining how people’s information is being used.”<sup>62</sup> According to this application’s

---

<sup>59</sup> Jeremy Kirk, *Instagram, Grindr, and more popular Android apps put user privacy at risk, researcher says*, PC WORLD, Sept. 8, 2014, <http://www.pcworld.com/article/2603900/popular-android-apps-fail-basic-security-tests-putting-privacy-at-risk.html> (regarding popular general audience apps rather than just those targeting children); *see also* Youtube, DAY 1: SECURITY ISSUES IN INSTAGRAM, OKCUPID, AND OOVVOO, <https://www.youtube.com/watch?v=FXQovCf-PfA&list=UUxdY4Hew6gdGblN6dV2eJbg&index=3> (the first of five videos detailing the many privacy problems with popular Android apps) (last visited Sept. 16, 2014).

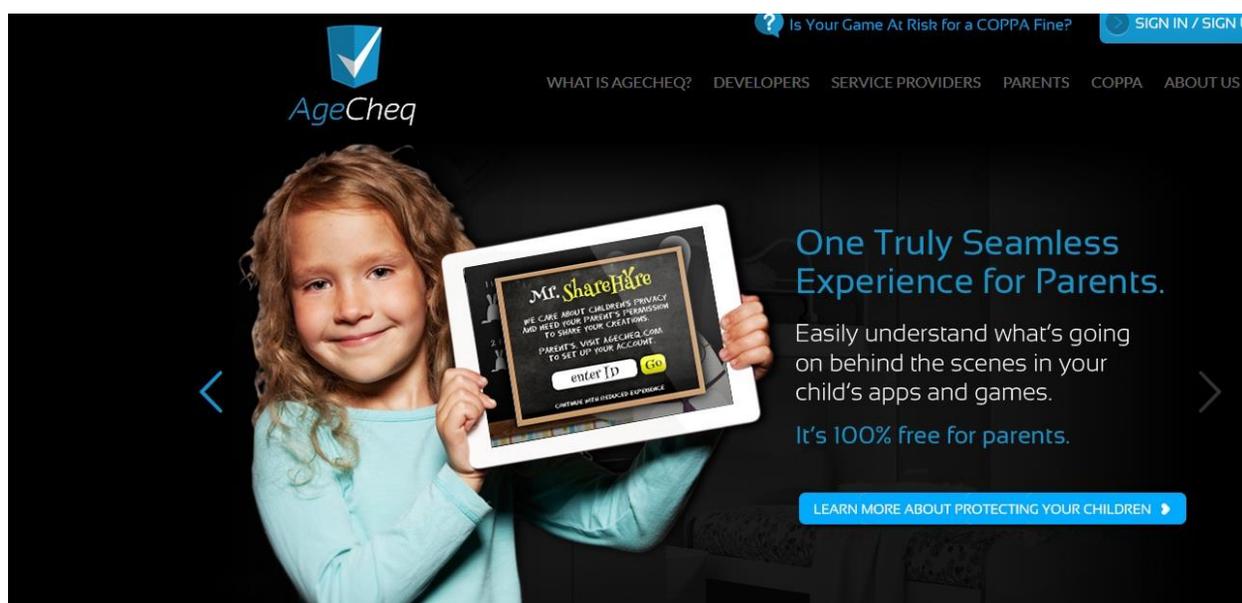
<sup>60</sup> FTC, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (December 2012), *available at* <http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf>; *id.* at 4 (“The survey results showed that parents still are not given basic information about the privacy practices and interactive features of mobile apps aimed at kids. Indeed, most apps failed to provide any information about the data collected through the app, let alone the type of data collected, the purpose of the collection, and who would obtain access to the data.”)

<sup>61</sup> News Release, United Kingdom Information Commissioner’s Office, Global survey finds 85% of mobile apps fail to provide basic privacy information, Sept. 10, 2014, *available at* [http://ico.org.uk/news/latest\\_news/2014/global-survey-finds-85-percent-of-mobile-apps-fail-to-provide-basic-privacy-information-20140910](http://ico.org.uk/news/latest_news/2014/global-survey-finds-85-percent-of-mobile-apps-fail-to-provide-basic-privacy-information-20140910).

<sup>62</sup> *Id.*

silence on the issue, AgeCheq makes no effort to help companies comply with these fundamental security and disclosure COPPA duties, not to mention other explicit duties under the law. As a result, its current assertions that it can get app developers into compliance with COPPA easily and for free—thus saving them from FTC fines—is a deceptive statement. Since the fines that these developers will incur could be hundreds of thousands of dollars,<sup>63</sup> it is beyond question that this deception is material to developers.

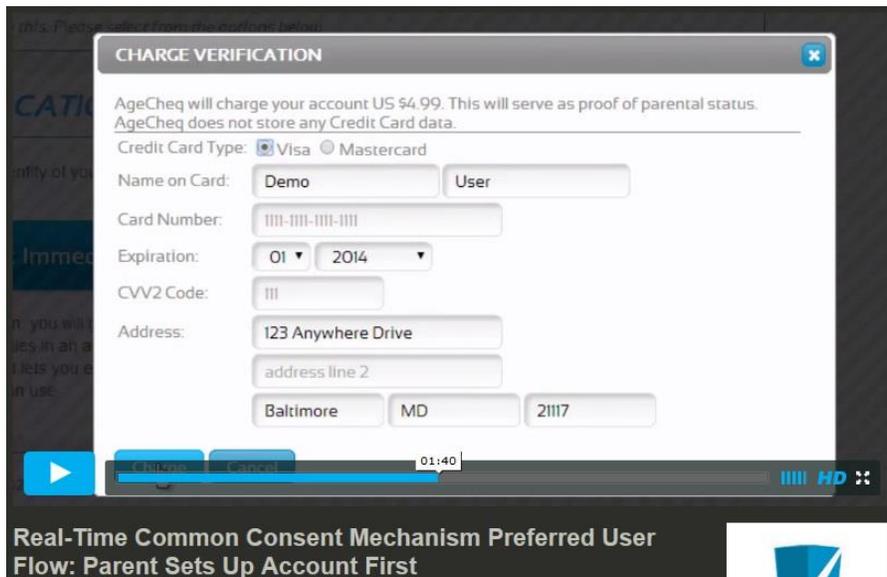
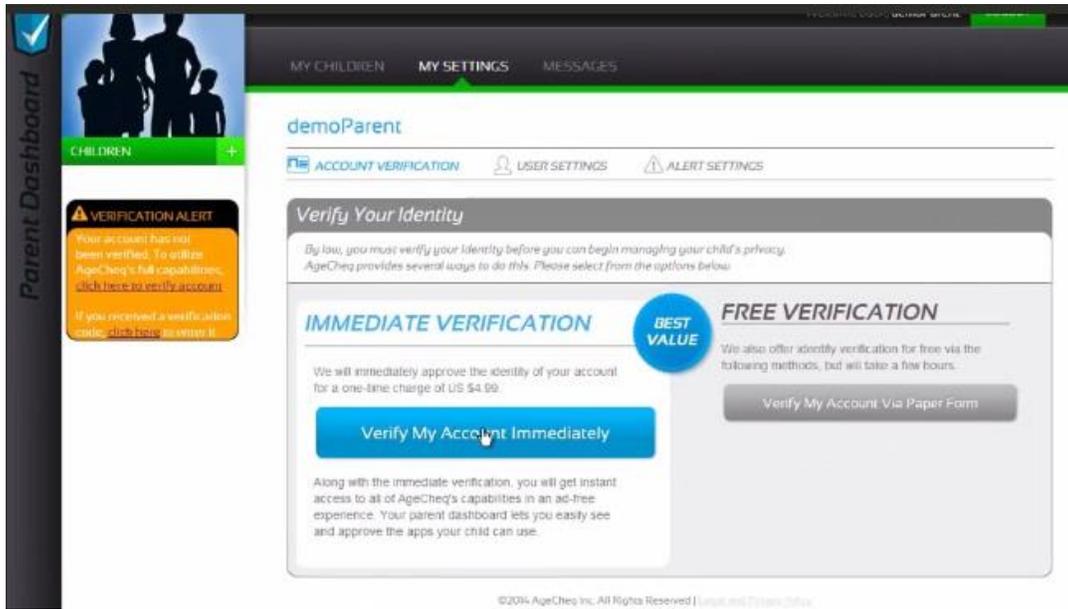
Another inexplicable deceptive statement by AgeCheq is that its homepage tells developers that its service is free to parents:



As discussed above, AgeCheq’s application to FTC affirms that the company is using credit card verification as its preferred VPC method (it also tells parents that this method is the “Best Value” although how that could possibly be true, as compared with what they call a “Free” option, is not

<sup>63</sup> Press Release, FTC, Yelp, TinyCo Settle FTC Charges Their Apps Improperly Collected Children’s Personal Information (Sept. 17, 2014), <http://www.ftc.gov/news-events/press-releases/2014/09/yelp-tinyco-settle-ftc-charges-their-apps-improperly-collected>.

clear from AgeCheq materials),<sup>64</sup> and several videos cited in the application show that parents will be charged five dollars for that type of verification.<sup>65</sup>



<sup>64</sup> See Vimeo, Real-Time Common Consent Mechanism Likely User Flow: Child Finds App First, <http://vimeo.com/agecheq/review/101104516/935919e707> (last visited Sept. 19, 2014) (briefly showing how AgeCheq presents its two VPC methods to parents inside its portal).

<sup>65</sup> See, e.g., Vimeo, Real-Time Common Consent Mechanism Preferred User Flow: Parent Sets Up Account First, <http://vimeo.com/agecheq/review/101104468/7e7ae4941c> (last visited Sept. 16, 2014).

The other option for parents to print and mail/fax/scan-and-email a form to AgeCheq also necessarily includes the costs of printing, mailing, and time expended. Neither VPC method is “100% free for parents,” and parents cannot use AgeCheq if they do not use one of these two methods. This deception is material to developers who make free children’s apps, because AgeCheq is saddling them with a non-free VPC method that many parents will not accept, while they might have accepted the developer’s own VPC innovation.

**b. AgeCheq’s proposal to mark devices as “parent” or “child” runs counter to FTC’s recent unfairness cases against unauthorized in-app purchases against app stores over-charging parents**

AgeCheq’s apparent Section 5 violations do not end with its deception of potential clients, it also may have based its parental re-identification model on a technology that violates unfairness standards articulated by FTC in recent cases against Apple, Google, and Amazon. These companies were sued in their capacity as app stores, centralized platforms that for the purposes of this analysis are equivalent to AgeCheq’s centralized COPPA platform covering numerous apps.

FTC has settled with Apple and Google for Section 5 violations related to the companies’ failure to stop children from circumventing parents’ consent to make in-app purchases in children’s apps.<sup>66</sup> Amazon has decided to go to court against FTC on similar charges.<sup>67</sup> In these

---

<sup>66</sup> Press Release, FTC, Apple Inc. Will Provide Full Consumer Refunds of At Least \$32.5 Million to Settle FTC Complaint It Charged for Kids’ In-App Purchases Without Parental Consent (Jan. 15, 2014), <http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million>; Press Release, FTC, Google to Refund Consumers at Least \$19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children’s Unauthorized In-App Charges (Sept. 4, 2014), <http://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it>

<sup>67</sup> Press Release, FTC, FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children’s Unauthorized In-App Charges (July 10, 2014), <http://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars>

cases FTC found a violation of the law when the app stores allowed a short window of time where children could make unlimited purchases after parents input passwords.<sup>68</sup> The unapproved purchases were discovered by parents when unexpected charges showed up on their credit card bills.<sup>69</sup>

Parents were bilked for tens of millions of dollars under the lax password policies of the app stores—AgeCheq’s system could be even easier to bypass. Worse than the sanctionable conduct FTC pursued in the above cases, AgeCheq’s application says it identifies a device as the “parent” and does not mention requiring a password or other proof of identity before that device can give a COPPA approval.<sup>70</sup> While the application never mentions passwords in conjunction with device-level re-identification,<sup>71</sup> one of the videos AgeCheq cites does show a parent using a password on a desktop browser,<sup>72</sup> leaving Commenters unsure of what parts of this common consent mechanism are protected and what parts are not. In contrast to that one video, AgeCheq’s terms of service suggest no password is needed after one VPC confirmation, because

---

<sup>68</sup> Apple allowed purchases for 15 minutes after a password input, Google allowed purchases for 30 minutes after password input. Press Release, FTC, Apple Inc. Will Provide Full Consumer Refunds of At Least \$32.5 Million to Settle FTC Complaint It Charged for Kids’ In-App Purchases Without Parental Consent (Jan. 15, 2014), <http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million>; FTC Complaint, In the Matter of Google, Inc. (undated document), <http://www.ftc.gov/system/files/documents/cases/140904googleplaycmpt.pdf>.

<sup>69</sup> See FTC Press Releases, *supra* notes 66, 67.

<sup>70</sup> App., *supra* note 2, at 9 (“We propose-and have developed-a device-based, real-time, platform-based method to associate parental identity with the device . . .”) (emphasis in original).

<sup>71</sup> See *generally id.*

<sup>72</sup> Vimeo, Real-Time Common Consent Mechanism User Flow For Typical Use After Initial Setup, <http://vimeo.com/agecheq/review/101104651/44bb720002> (last visited Sept. 16, 2014).

the company relies on a persistent cookie to forever mark the computer's browser as verified.<sup>73</sup> Lack of password protection on some devices could affect multiple "parent" access points as AgeCheq's application says it assumes parental identity by use of a device alone: "linking a verified parental identity to a specific device . . ." <sup>74</sup> which does not even have to be a single dedicated device, as one flowchart says parents can approve any request "[u]sing the most convenient method (desktop, tablet, smart phone) . . ." <sup>75</sup> The company is apparently proud that it is using device identification technology, which constitutes illegal tracking under COPPA, as the main form of re-identification of parents and children.<sup>76</sup> Unlike the in-app purchases example, however, parents will get no bank statement to warn them that their child's privacy has been violated—the COPPA disclosure and choice to approve collection will have already passed with no other notice normally sent to the parent. Amazingly, while it seems that children always receive notifications that would encourage them to spoof a parental account, the AgeCheq application demonstrates that *it does not know* if parents will receive notifications that a child is trying to use a relevant app.<sup>77</sup> AgeCheq's system never asks a child for their parent's contact

---

<sup>73</sup> "An example of a persistent cookie is one that tells us you have already authenticated your identity with us and are not required to do so again." AgeCheq legal and privacy policy information, [http://www.agecheq.com/?page\\_id=217](http://www.agecheq.com/?page_id=217) (last visited Sept. 22, 2014).

<sup>74</sup> App., *supra* note 2, at 10.

<sup>75</sup> *Id.* at 16 (Figure 5).

<sup>76</sup> "As the Commission has recognized, the unique identifiers associated with a device can be used to track its use across online services." *Id.* at 11 (citing the FTC statement of basis and purpose explaining why such identifiers are personal information under COPPA).

<sup>77</sup> Compare "the app alerts the child that parental permission is required" with "The RCCM *could also integrate* other notification options, such as parental alerts via email or SMS text message." (emphasis added) *Id.* at 12–13. According to some of AgeCheq's flow charts, such notification might be available as an opt-in, but the flow charts affirmatively do not describe AgeCheq's actual practices. *See id.* at 16 (Figure 5); *id.* at 13–14 (explaining that its flow charts do not describe the AgeCheq business plan but a hypothetical common consent mechanism that any company might use). In contrast to the actual application, one of the videos the company cites to says AgeCheq allows parents to opt-in to email and text notifications. Vimeo, Real-Time

information, instead relying on a message to the child (on what will be tracked as the “child” device) to initiate VPC with an adult.<sup>78</sup> As a result, this identification system is significantly worse than the in-app purchases cases on two metrics: rather than requiring a parent’s password and providing a short window where children could pose as parents as the app stores did, AgeCheq potentially allows this to happen at all times of the day and night through multiple “parent” devices; also, parents will not receive an independent warning that such fraud has occurred.

It seems that AgeCheq’s system is a tax on regular parents, paid for in harm to their children’s privacy. The company apparently assumes that every parent will have the means to buy each of their children personal devices, not to mention the time to constantly monitor children when they are near the “parent” devices that might not be password protected. When an app joins AgeCheq, the common consent mechanism is presented to parents as a take-it-or-leave-it whole, so parents who might allow their children access to games on the “parent” device or might have other concerns than constantly monitoring devices and children are simply out of luck under the AgeCheq platform. Parents who cannot afford many dedicated mobile devices, and who do not lock their “parent” devices, are harmed by AgeCheq’s assumptions and slack re-identification standards, because these parents have no good way to stop children from approving apps through the flawed AgeCheq service. This is not appropriate under the law, and the fact that

---

Common Consent Mechanism User Flow For Typical Use After Initial Setup,  
<http://vimeo.com/agecheq/review/101104651/44bb720002> (last visited Sept. 16, 2014).

<sup>78</sup> See *id.* at 15 (Figure 4); see also Vimeo, Real-Time Common Consent Mechanism Likely User Flow: Child Finds App First, <http://vimeo.com/agecheq/review/101104516/935919e707> (demonstrating that the system never asks for a parent’s contact information and so it is entirely up to the child to make the parent set up a parent account, or just as likely set up one of his own) (last visited Sept. 19, 2014).

this platform is already on the market<sup>79</sup> suggests that this faulty method of identifying parents is already creating the potential for many apps to collect child information in violation of COPPA. Unlike the in-app purchases settlements, no money damages will make these parents whole after their children's information is collected without valid VPC.

**c. AgeCheq's submission demonstrates that it is an operator under COPPA collecting personal information from children without complying with COPPA's notice requirements**

Despite the fact that AgeCheq claims to be an expert on COPPA compliance it does not comply with COPPA even though it is bound to do so. The company is an operator collecting personal information from those it has actual knowledge are children, yet it does not have a COPPA-complaint privacy policy and its videos that are meant to demonstrate the parent experience show no just-in-time COPPA notification of AgeCheq's practices.<sup>80</sup>

AgeCheq is squarely within COPPA's definitions. An "operator" is "any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service . . ."

§ 312.2 "Personal information:"

means individually identifiable information about an individual collected online, including: . . . (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier . . . (10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

---

<sup>79</sup> "Importantly, the proposed method is not only feasible—it is available today." *Id.* at 13.

<sup>80</sup> *See, e.g.*, Vimeo, Real-Time Common Consent Mechanism Preferred User Flow: Parent Sets Up Account First, <http://vimeo.com/agecheq/review/101104468/7e7ae4941c> (last visited Sept. 19, 2014).

§ 312.2. “Collection” includes “[p]assive tracking of a child online.” § 312.2. Hence, as AgeCheq tracks children’s devices using the internet and logs their usage of apps, with technologies that are never fully explained in the instant application and only briefly alluded to in the company’s privacy policy video (discussed below), it is collecting personal information from children as an operator. Once these factors are established: “It shall be unlawful for any operator . . . that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the” COPPA Rule, including COPPA’s requirements for: notice; VPC; parental review and ability to refuse further collection or information use; not conditioning child’s participation on over-collection of information; and data security and integrity standards. § 312.3. AgeCheq should be investigated for violations under all these duties.

Despite the fact that AgeCheq denies this,<sup>81</sup> the videos showing the use of its service cited to in the application show what is “likely” to be a *child* initiating a process that collects the child’s persistent identifier and starts to track it.<sup>82</sup> AgeCheq knows that all such persistent identifiers it collects are coming from child-directed online services, since those are the only operators that will join its common consent mechanism. The fact that the parent later confirms that the persistent identifier belongs to a child<sup>83</sup> does not mean that it was collected from the parent, it just confirms that AgeCheq has obtained actual knowledge that it has already collected

---

<sup>81</sup> “We do not knowingly solicit personal information from anyone under the age of 13 or knowingly allow such persons to register for our services.” AgeCheq legal and privacy policy information, [http://www.agecheq.com/?page\\_id=217](http://www.agecheq.com/?page_id=217) (last visited Sept. 22, 2014).

<sup>82</sup> See, e.g., Vimeo, Real-Time Common Consent Mechanism Likely User Flow: Child Finds App First, <http://vimeo.com/agecheq/review/101104516/935919e707> (last visited Sept. 19, 2014).

<sup>83</sup> See *id.*

a persistent identifier from a child. Despite all this, the company does not provide parents with proper notice under § 312.4.

AgeCheq's privacy policy violates COPPA in several ways. Generally speaking, it is the combination of the company's terms of service and the privacy policy,<sup>84</sup> so it is full of extraneous information that does not relate to privacy in violation of § 312.4 (a) ("It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials."). Although it shares users' personal information with third party service providers<sup>85</sup> AgeCheq never names them in violation of § 312.4(d)(1). The company says it does not collect personal information from anyone under 13,<sup>86</sup> despite the fact that COPPA covers collecting "[i]nformation concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier . . ." § 312.2, which is not only AgeCheq's practice but a central part of its business model.<sup>87</sup> The company redefines personal information

---

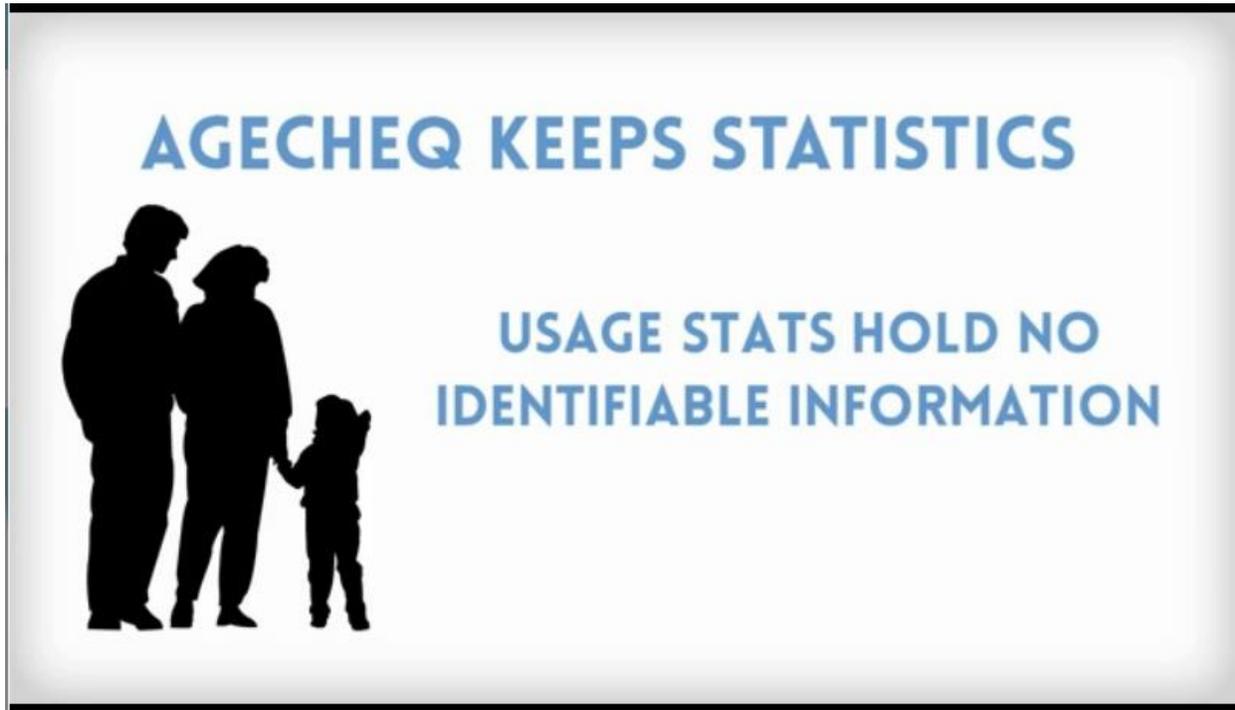
<sup>84</sup> AgeCheq legal and privacy policy information, [http://www.agecheq.com/?page\\_id=217](http://www.agecheq.com/?page_id=217) (last visited Sept. 22, 2014).

<sup>85</sup> "When you create a parent account on the AgeCheq Service, COPPA regulations require us to have a 'Positive Identification' that you are in fact who you claim to be. To facilitate this, we use a third party service provider to verify your identity. In the course of verifying your identity, your personal information may be disclosed to this third party service provider."

<sup>86</sup> "We do not knowingly solicit personal information from anyone under the age of 13 or knowingly allow such persons to register for our services." AgeCheq legal and privacy policy information, [http://www.agecheq.com/?page\\_id=217](http://www.agecheq.com/?page_id=217) (last visited Sept. 22, 2014).

<sup>87</sup> "Under the proposed [common consent mechanism], this verified identity is linked to a secure parent account, which in turn is linked to device(s) used by the parent's children. As the Commission has recognized, the unique identifiers associated with a device can be used to track its use across online services." App., *supra* note 2, at 11. "It is a highly scalable method that can be used across incompatible device platforms and which uniquely follows the Commission's lead by tying verified identities to individual devices." *Id.* at 17.

to suit its needs, claiming in its privacy video<sup>88</sup> (ostensibly a summary of the privacy policy, but containing different information that is not laid out in the written policy)<sup>89</sup> that usage data tied to child accounts is not personal information and therefore is not harmful to privacy:



---

<sup>88</sup> Vimeo, AgeCheq's Demonstration Marquee Explainer Video, <http://vimeo.com/92159923> (last visited Sept. 22, 2014).

<sup>89</sup> Compare *id.* with AgeCheq legal and privacy policy information, [http://www.agecheq.com/?page\\_id=217](http://www.agecheq.com/?page_id=217) (last visited Sept. 22, 2014).

The written company privacy policy makes no mention of this tracking on mobile devices, it only mentions two types of cookies that AgeCheq uses for browser-based tracking.<sup>90</sup> The company's privacy policy video also states that it only collects information required by COPPA and then lists all of the many items of personal information it requires from parents (which it retains indefinitely and does not use for VPC) that are not required by COPPA:



---

<sup>90</sup> “We use cookies to track your session information in order to improve your AgeCheq Service experience and the quality of our services. A cookie is a small text file that is stored on a user’s computer for recordkeeping purposes. We link information we store in cookies to personal information you submit while using the AgeCheq Service.” AgeCheq legal and privacy policy information, [http://www.agecheq.com/?page\\_id=217](http://www.agecheq.com/?page_id=217) (last visited Sept. 22, 2014).

## PARENT ACCOUNTS:



IDENTIFY YOUR DEVICE  
YOUR NAME  
ADDRESS  
PHONE NUMBER  
EMAIL ADDRESS  
BIRTH MONTH / YEAR  
LAST 4 SSN DIGITS

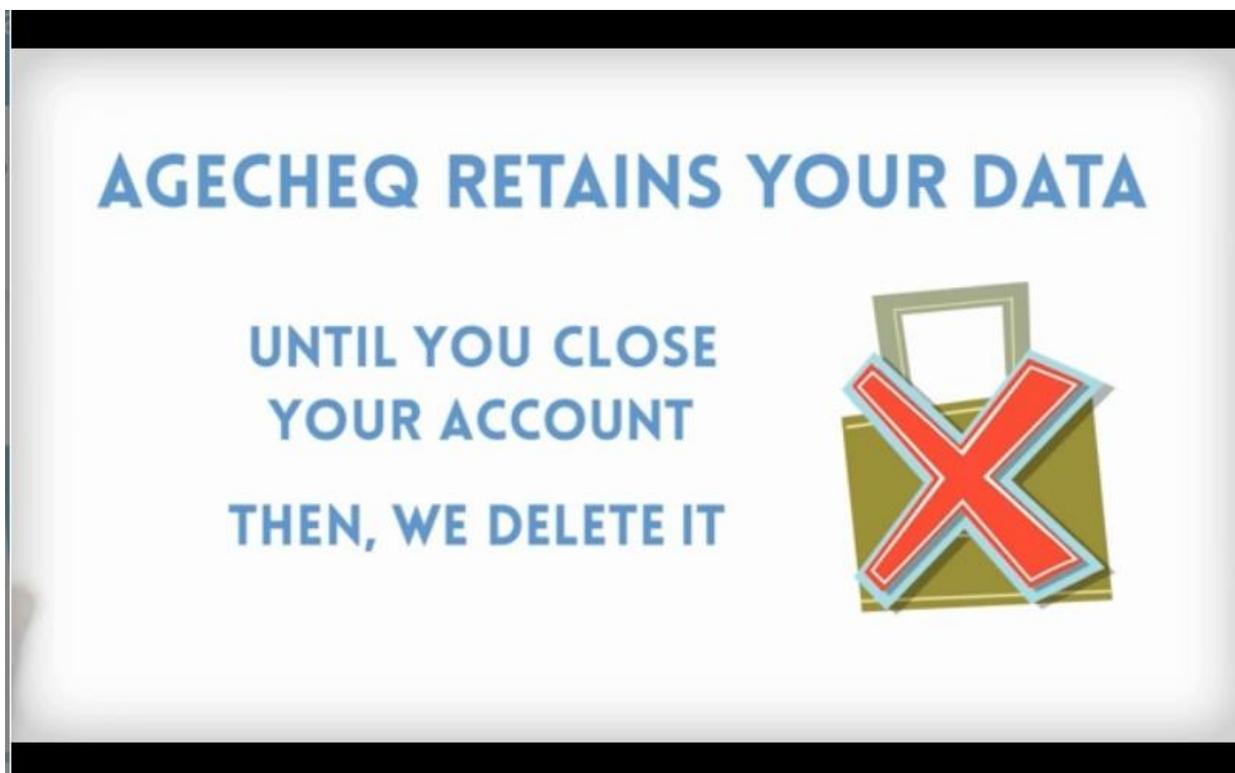
Both the company's privacy policy and the "summary" video containing different information claim that the company does not collect any personal information from children, which violates § 312.4(d)(2) by not explaining the collection of usage statistics from children that it ties to personal information:

# AGECHEQ NEVER COLLECTS

## ANY INFORMATION FROM YOUR CHILDREN



The company's video reveals that parents do not have an option to review or selectively delete personal information collected from their children (required under § 312.6; disclosure in privacy policy required under § 312.4(d)(3)), the only option is a take-it-or-leave it approach where a parent has to delete all family accounts to try to stop AgeCheq from profiling a child:



The company's own application demonstrates how it is violating COPPA. AgeCheq's history lesson on COPPA contains a full page and a half discussion of how it is illegal under COPPA to track children using persistent identifiers,<sup>91</sup> then twice in its application it indicates that it is using such identifiers to track children.<sup>92</sup> This company claims to its customers that it is an expert in COPPA compliance,<sup>93</sup> while at the same time it tries to write its privacy policy in a way that sidesteps the fact that it is tying children's device identifiers to account information and to usage statistics.

AgeCheq's application notes that it has an unmatched technological ability to track children: "It is a highly scalable method that *can be used across incompatible device platforms* and which uniquely follows the Commission's lead by tying verified identities to individual

---

<sup>91</sup> See App., *supra* note 2, at 6–7.

<sup>92</sup> *Id.* at 11, 17.

<sup>93</sup> See Section II.a, *supra*.

devices.”<sup>94</sup> (emphasis added). The company’s ability to track what apps a child uses, when they use them, and possibly the location of the child while they are using the apps (i.e. through IP address or cell tower information) goes far beyond the abilities of any app developer to track a child over time and across different Web sites or online services—this is potentially a full profile of a child’s preferences and habits, which AgeCheq says it will provide to third parties<sup>95</sup> when it has been made “anonymous or aggregated.”<sup>96</sup> The fact that the company uses “or” between “anonymous *or* aggregated” allows it to sell the information of individual children that is “anonymous” or non-anonymous batches of children, both of which are inappropriate policies for a company that is trying to be the central gateway for COPPA compliance.<sup>97</sup>

### **III. This Administrative Proceeding is Arbitrary and Capricious, an Abuse of Discretion, and Not in Accordance With the Law**

AgeCheq’s application to FTC is a farce. By repeating it, the Commission makes a mockery of the Administrative Procedure Act (APA). Rather than investigating a company that

---

<sup>94</sup> App., *supra* note 2, at 17.

<sup>95</sup> “We may share aggregated and anonymized information with any third party in a form that does not directly identify you. By using the AgeCheq Service you acknowledge and consent to such use.” AgeCheq legal and privacy policy information, [http://www.agecheq.com/?page\\_id=217](http://www.agecheq.com/?page_id=217) (last visited Sept. 22, 2014).

<sup>96</sup> “We do not consider personal information to include information that has been made anonymous or aggregated so that it can no longer be used to identify a specific person.” AgeCheq legal and privacy policy information, [http://www.agecheq.com/?page\\_id=217](http://www.agecheq.com/?page_id=217) (last visited Sept. 22, 2014).

<sup>97</sup> Press Release, AgeCheq supports over 400 million app starts per day as FTC COPPA enforcement leaves game publishers scrambling to comply with 2012 law (Sept. 24, 2014), *available at* <http://www.mobilitywire.com/agecheq/2014/09/24/8498> (“‘We designed our cloud infrastructure to massively scale in support of the millions of app starts we will see as top games use our compliance service,’ added [AgeCheq CEO] Smith. ‘Today, our backend can comfortably handle 5,000 app starts per second, which translates to over 430 million app starts per day. By the beginning of 2015, we’ll be able to process over 1 billion app starts per day.’”).

is undercutting and harming COPPA compliance with an assortment of deceptive and unfair practices, FTC decided to help this company by publicizing its product through this notice and comment proceeding. Approving this application would make FTC complicit in this company's deceptive and unfair practices.

First of all, as outlined above, basic research within the four corners of this application and on AgeCheq's website reveals that it is potentially: deceiving app developers into thinking it is a COPPA Safe Harbor, and mischaracterizing the extent of COPPA so that they unknowingly violate it; causing its clients to violate COPPA by providing parents with incomplete and confusing disclosures, and not giving parents their due under the law to refuse access; basing its entire system on a parental re-identification model that could be worse than the unfair practices FTC has fought against in child-directed apps in major app stores; and making other deceptive statements to potential app developer clients in order to get them to adopt a technology that will charge parents money before their children can use developers,' largely free, apps.<sup>98</sup> Did FTC do any research into this company before initiating this notice and comment process? If so, it is unbelievable that the problems found here (many of which are in the materials provided by AgeCheq, such as the videos they cite as support) did not alert the Commission's staff to a potential raft of violations, deserving of a formal investigation. If FTC did do the basic research necessary to vet this submission, did it find these violations and go ahead with the notice and comment process concurrently to a formal investigation? Commenters are left wondering.

---

<sup>98</sup> While not all children's games are free, the vast majority of them are, and AgeCheq is targeting "small businesses and even individuals" rather than large media companies that can sell apps based on established children's content that is already popular in the market. App., *supra* note 2, at 5.

Secondly, this process is unsound from the start because there is no basis in the public record upon which FTC could approve this application. According to the APA, in rulemaking FTC must cite the legal basis for the rule and notify the public of “either the terms or substance of the proposed rule or a description of the subjects and issues involved.” 5 U.S.C. § 553(b)(2)–(3). Both COPPA and FTC’s notice of this comment period specify: “*To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with analysis of how the methods meet § 312.5(b)(1),*” § 312.12(a) (emphasis added).<sup>99</sup> FTC is currently considering the application without such a showing. There is no new VPC method proposed in this submission, it relies on pre-approved VPC methods to verify parental identity. Assuming FTC’s staff somehow overlooked AgeCheq’s assertions that it was proposing to use only existing methods, the application is still deficient. Rather than providing specifications of its re-identification technology, or other relevant detail, this application is at pains to summarize the history of COPPA before then describing the proposed method with at a high level of generality with no further support. More than half the seventeen pages are taken up with superfluous information, while the actual “proposed verification method for mobile devices” section lacks substance and citation to authority. Commenters are given no specifics about what AgeCheq is proposing. Is the parent gateway password protected? What is so secure about a “secure parent account?”<sup>100</sup> How does the company employ “the unique identifiers associated with a device [that] can be used to track its use across online services?”<sup>101</sup> Commenters do not dispute the fact that this *can* be done, but nowhere in this application is a “detailed description” of how it will be done or if it will work. The application never gives

---

<sup>99</sup> See also similar language in VPC Notice, *supra* note 1, at 51514.

<sup>100</sup> *Id.* at 11.

<sup>101</sup> *Id.*

Commenters “the substance of the proposed rule” that should be apparent in such a rulemaking notification.

FTC has approved redacted and paltry submissions in the past, and Commenters have been asked to comment on company submissions that are weak to the point of being nearly pointless.<sup>102</sup> However this application is uniquely deficient. FTC needs to face up to that fact and admit that it is asking the public to comment on meritless applications. As AgeCheq merrily noted in its history lesson: “For the Commission, charged by law with enforcing COPPA, this ‘scofflaw’ climate is frustrating, but hard to counteract with limited enforcement resources.”<sup>103</sup> Why FTC is using these limited resources to indulge applications that come nowhere near the basic requirements of COPPA is beyond Commenters. Without a change in course FTC risks taking arbitrary and capricious agency action that cannot be justified under the law. *See* 5 U.S.C. § 706(2)(a). This does a disservice to the Commission as well as the future of children’s online privacy.

---

<sup>102</sup> *See* Imperium submissions to FTC, two documents covering a total of seven pages, redacted in the part that actually discussed the effectiveness of the proposed method. Imperium, Second Revised 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), Aug. 12, 2013, <http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-seeks-public-comment-imperium-llc-proposal-parental-verification-method-under-coppa-rule/130909imperiumapplication.pdf>; Imperium, Responses to FTC Questions Regarding Imperium Pursuant to COPPA Rule Section 312.12(a) for Approval of Parental Consent Method Not Currently Enumerated in Section 312.5(b), Sept. 13, 2013, <http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-seeks-public-comment-imperium-llc-proposal-parental-verification-method-under-coppa-rule/130909imperiumresponsestoftc.pdf> (significant part of Imperium’s response to FTC questions redacted on page 2). FTC subsequently approved this application with no other showings on the public record.

<sup>103</sup> App., *supra* note 2, at 8.

## CONCLUSION

For the reasons stated above FTC should not approve this application and should open a full investigation of AgeCheq for its Section 5 violations, as well as its violations of COPPA. If the Commission finds that the company has caused its clients to violate COPPA due to its deception and failure to create a valid common consent mechanism, FTC should hold the company jointly liable for any fines assessed to the operators who have relied on promises that it will shield them from enforcement actions.

Signatory:

/s/  
\_\_\_\_\_  
Hudson B. Kingston  
Legal Director  
Center for Digital Democracy  
1621 Connecticut Ave., NW  
Suite 550  
Washington, DC 20009  
(202) 986-2220

/s/  
\_\_\_\_\_  
Josh Golin  
Associate Director  
Campaign for a Commercial-Free Childhood  
NonProfit Center  
89 South St., # 403  
Boston, MA 02111  
(617) 896-9369

September 30, 2014