REDACTED FOR PUBLIC INSPECTION

ORIGINAL

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

July 25, 2014

Re: 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)

Dear Mr. Clark:

Pursuant to Section 312.12(a) of the Final Children's Online Privacy Protection Rule (the "Rule"), AgeCheq Inc. ("AgeCheq") hereby requests Federal Trade Commission ("Commission") approval of a parental verification method, not currently enumerated in the Rule. The proposed method allows a parent to curate a child's mobile application ("app") experience in real-time, through automated, device-level, implementation of verified parental consent. As implemented by AgeCheq, the proposed common consent mechanism method is tightly integrated with certain ancillary services provided on behalf of developers and parents, which facilitate the entire range requirements under the Children's Online Privacy Protection Act, such as notices, permissions, in-app gates, and revocation communication between parents, mobile app developers, and advertising networks, through the use of mobile device and cloud-based web technology. The proposed method incorporates, but uniquely extends, tried and true

(legacy) methods to verify parental identity by permitting real-time, device-specific verified enrollment of parents and of the associated child's devices in a robust common notice and consent management platform designed to serve an unlimited number of mobile applications (or websites).

SUMMARY OF PROPOSED METHOD

AgeCheq seeks FTC approval of a single identity verification process fulfilled through a common consent mechanism administered by a third party, as depicted more completely below and in the accompanying materials, but summarized as follows:

- A parent personally registers him/herself and the child's device(s) with a third party common consent administrator ("CCA");
- The CCA verifies parental identity through any currently enumerated method; and
- The CCA technically links that verified identity with the mobile devices used by their children, thereafter allowing app-specific permission to be granted to (or revoked from) each individual device.
- Meanwhile, participating developers embed code within their apps which automatically query the CCA's database to ensure parental consent has been granted. If consent has not yet been granted, a verified parent must use the CCA service to review the developer's app-specific privacy disclosures and affirmatively grant consent.

This method (more fully explained below) achieves the Commission's vision of a reliable, manageable, parent-curated online experience for children who use smartphones, tablets, or PCs to interact with mobile applications or other online services.

BACKGROUND

The Children's Online Privacy Protection Act ("COPPA" or the "Act") was enacted by Congress to protect children under the age of 13 from the unauthorized collection or use of their

personally identifiable information.[1] After the passage of COPPA in 1998, the Commission issued its final Rule in 1999, which became effective on April 21, 2000.[2] The Commission amended the Rule in 2012 and these amendments became effective on July 1, 2013.[3] The Act applies to the operators of certain "website[s] or online service[s]," but neither term is defined by statute.[4] The Act delegates the Commission general authority to issue implementing regulations to give meaning to the Act.[5] Using that authority, the Commission has stated that these terms are to be "broadly understood," noting that past commenters have "expressed a consensus that both the COPPA statute and Rule are written broadly enough to encompass many new technologies."[6]

When COPPA was enacted, "websites" and the "Internet" were still new to most Americans. When COPPA was drafted and passed in 1998, the first iPhone was still nine years away.[7] Children accessed online content via stationary computers, connecting to domains on the World Wide Web, or logging in to "walled garden" "online services," such as America Online, Prodigy or Compuserve. Some of this content was specifically designed for, or collected information from, children and therefore these services were covered as an "online service" under COPPA. The enumerated methods for verifying that the child's parent had notice of, and had consented to, a website's collection, sharing, and use of personally identifiable information

1 15 U.S.C. §§ 6501–6506. Note that throughout we use the terms "child" and "children" as the statute does, to mean "an individual under the age of 13." *See* 15 U.S.C. § 6501(1).

2 16 C.F.R. § 312.

3 16 C.F.R. § 312.12(a).

4 15 U.S.C. § 6502(a)(1).

5 15 U.S.C. § 6502(b). Moreover, COPPA, having been passed as part of an omnibus appropriations bill, leaves sparse legislative history, including little mention in the conference report. *See* H. Conf. Rep. 105-825 at 754.

6 76 Fed. Reg. 59,807 (2011).

7 *See* Wikipedia, *iPhone*, *available at* http://en.wikipedia.org/wiki/IPhone.

about the child were straightforward (if limited), and the burden on parents (receiving a copy of a notice by email) manageable. The crux of COPPA's protections is the requirement that an operator "obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children." Verifiable parental consent, as set forth in the Rule, means that operators must use a consent method that is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. Enumerated or approved methods to date include: using a print-and-send form that can be faxed or mailed back to the operator; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using email accompanied by a PIN or password obtained through one of the above methods.[8]

Just fifteen years after its passage, the online life of a child under 13 has expanded and evolved in unforeseen ways, greatly complicating the challenges for parents needing to curate their child's online life, and the thousands of developers with whom children can potentially interact online via apps on smartphones or tablets. On a macro level, today's mobile market bears little or no resemblance to the "online services" which existed in 1998. The walled garden of managed online services has given way to "wide open spaces"—millions of unique apps, each with its own practices related to personal information.[9] On a micro level, however, each app is

8 16 C.F.R. § 312.5(b)(2).

9 *See* Tech Crunch, "iTunes App Store Now Has 1.2 Million Apps, Has Seen 75 Billion Downloads To Date" (June 2, 2014), *available at* http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/ (reporting that Apple announced that its App Store has 1.2 million apps available for download); *see also* Tech Crunch, "Google Play Quarterly App Revenue More Than Doubled Over Past Year, Thanks To Games, Freemium Apps" (June 24, 2014), *available at* http://techcrunch.com/2014/06/23/google-play-quarterly-app-

its own walled garden, providing access to a closed universe of content and features. The ubiquity of the universal web browser has expanded to include a fragmented ecosystem of single purpose apps, many of which have been developed and promoted by small businesses and even individuals. The business models for supporting online offerings for children have been transformed by the advent of advertising targeting and tracking devices and users over time and across these online activities. The use of mobile devices by children has exploded,[10] as has the number of developers creating content.[11] As of June 2014, Apple's App Store surpassed 75 billion downloads, with 19 out of the 25 most popular apps being games (many of which are popular with children).[12] Google Play announced its 50 billionth download more than a year ago, further demonstrating how broadly the mobile ecosystem has emerged in so little time.[13] In short, new technologies and new online offerings, supported by new means to track and monetize through third party ad networks have created new COPPA-driven challenges for parents, developers, and networks alike.

revenue-more-than-doubled-over-past-year-thanks-to-games-freemium-apps/ (noting that the Google Play store has "well over 1 million apps").

10 *See* Kleiner Perkins Caufield Byers, *Internet Trends Report* (Dec. 3, 2012), *available at* http://www.slideshare.net/kleinerperkins/2012-kpcb-internet-trends-yearend-update (noting that 29% of adults now own a tablet computer, up from less than 2% three years earlier).

11 *See* Vision Mobile, *App Economy Forecasts 2013-2016* (July 2013), *available at* http://www.visionmobile.com/product/app-economy-forecasts-2013-2016/ (predicting that there will be approximately 5 million app developers globally by 2016).

12 *See supra* note 9; Forbes, "Apple: As The App Store Nears 50 Billion Downloads, The Birds Remain Angry (And Popular)" (May 3, 2013), *available at* http://www.forbes.com/sites/markrogowsky/2013/05/03/apple-as-the-app-store-nears-50-billion-downloads-the-birds-remain-angry-and-popular/.

13 The Verge, "Google: Android app downloads have crossed 50 billion, over 1M apps in Play" (July 24, 2013), *available at* http://www.theverge.com/2013/7/24/4553010/google-50-billion-android-app-downloads-1m-apps-available.

These challenges came to the fore in 2011 when the Commission explicitly determined that apps offered in app stores for download to smartphones and tablets fell within the scope of "websites and online services."[14] Therefore, the developers of those apps are "operators" subject to the requirements of COPPA.[15] The advent of tablets and smartphones also required consideration of the reach of the definition of "personal information" to explicitly include persistent identifiers tied to the device, not merely the data elements specifically enumerated in the statute, such as name and contact information. The Rule now includes "persistent identifier[s] that can be used to recognize a user over time and across different Web sites or online services" within the definition of personal information.[16] Among the examples of persistent identifiers recognized as personal information by the Commission are an "Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."[17] These identifiers are a significant change from prior COPPA rules, which focused on the collection of personal information that was unrelated to the user's device. These new rules specifically target the gathering of information that is tied to individual pieces of hardware, such as mobile phones. The Commission undertook this expansion in response to what it recognized as the "shift" in consumer habits from "a single, family-shared, personal computer to the widespread distribution of person-specific, Internet-enabled, handheld devices to each member within a household,

14 76 Fed. Reg. 59,807 (2011) (noting that the term "broadly covers any service available over the Internet, or that connects to the Internet or a wide-area network," including a "host of current technologies," such as mobile applications, Internet-enabled gaming platforms, voice-over-Internet Protocol, and Internet enabled location based services).

15 16 C.F.R. § 312.2 (defining an "operator" as "any person who operates a Web site located on the Internet or an online service ...").

16 *Id.*

17 *Id.*

including children."[18] Whereas an earlier evolution of the Rule broadly allowed for the collection of these identifiers for "internal support" functionality, the new Rule closes that door whenever the device information is being used for the purpose of "amassing data on a child's online activities or behaviorally targeting advertising to the child."[19] In this way, the introduction of third party automated, targeted ads to users of apps, on the basis of device-based persistent identifiers, prompted further expansion of COPPA's reach. Developers who utilized third party ad delivery networks which track by persistent device-based identifiers are deemed to have "contacted" the child, such that verified (pre-collection) parental consent is required.

The combination of these marketplace and regulatory developments have created significant inefficiencies and compliance burdens. To accomplish the required parental verification and obtain consent is such a daunting challenge, that even developers targeting children may ignore the requirements and instead assume the risk of enforcement attention as a cost of doing business.[20] In February 2012, the Commission released its findings after having studied 400 apps for children. The report found app developers offered little or no information to parents about their privacy practices and proclaimed itself a "warning call to industry" that it must do more."[21] Ten months later a second report followed, announcing that "most apps failed to provide any information about the data collected through the app, let alone the type of data

18 76 Fed. Reg. 59,812 (2011).

19 *Id.*

20 *See* Entertainment Software Association (comment 32, 2012 SNPRM) at 2 (noting that many game publishers avoid offering services to children due to COPPA regulations); P. Aftab (comment 1, 2012 SNPRM) at 3 (for operators, "confusion abounds"); and Association for Competitive Technology (comment 5, 2011 NPRM) at 3 (highlighting that "the requirements for parental consent are difficult and costly").

21 *See* FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), at 2.

collected, the purpose of the collection, and who would obtain access to the data."[22] Taken together, these reports are strong evidence of a disconnect between the expectations of the Rule and practices in the marketplace. For the Commission, charged by law with enforcing COPPA, this "scofflaw" climate is frustrating, but hard to counteract with limited enforcement resources.

In varied public statements, the Commissioners and Commission staff have expressed an eagerness to mitigate the operational and compliance burdens for parents and developers alike, through **common consent mechanisms,**[23] and other platform-based consent delivery and management systems. When the Commission revisited the COPPA Rule in 2013, it specifically addressed the methods for obtaining consent. The amended rule authorized an interested party to file a written request for Commission approval of parental consent methods not currently enumerated.[24] While the Commission did not approve any such platforms along with the Rule, it did expressly encourage the continued development of these methods.[25] The interested party must provide a detailed description of the proposed parental consent method, together with an

22 *See* FTC Staff, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012), http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.

23 78 Fed. Reg. 3,989 (2013).

24 16 C.F.R. § 312.12(a).

25 78 Fed. Reg. 3,989 (2013); *see also* CDT (comment 15, 2012 SNPRM) at 5–6 (noting that, with clear terms and robust controls, "it may be reasonable to allow the third party applications to outsource COPPA compliance" to a platform); ESA (comment 47, 2011 NPRM) at 21–26 (supporting common consent methods operated by a game console); Facebook (comment 33, 2012 SNPRM) at 18 (calling for an "explicit clarification that operators can use a common mechanism, such as one provided by a platform in which multiple operators participate, to provide notice and obtain verifiable parental consent"); Future of Privacy Forum (comment 55, 2011 NPRM) at 5–6 (calling for a Commission approval of a third party mechanism, while urging that the operator retains primary responsibility for COPPA compliance); Microsoft (comment 107, 2011 NPRM), at 13–15 (supporting the use of a common mechanism to reduce "complexity); and The Walt Disney Co. (comment 170, 2011 NPRM), at 17–19 (noting that the "shift away from direct access to each individual website and online service necessitates the creation of new parental outreach and consent mechanisms that leverage these cooperative service delivery technologies").

analysis of how the method meets the requirements for parental consent described in 16 CFR § 312.5(b)(1).[26] The Commission stated that it "believes that common consent mechanisms, such as a platform, gaming console, or a COPPA safe harbor program, hold potential for the efficient administration of notice and consent for multiple operators."[27] Therefore, the Commission invited parties such as AgeCheq to "participate in the voluntary Commission approval process," which would enable the Commission to evaluate, and other interested parties to publicly comment upon, such proposals in an effort to bring to market sound and practical solutions that will serve a broad base of operators.[28]

PROPOSED VERIFICATION METHOD FOR MOBILE DEVICES

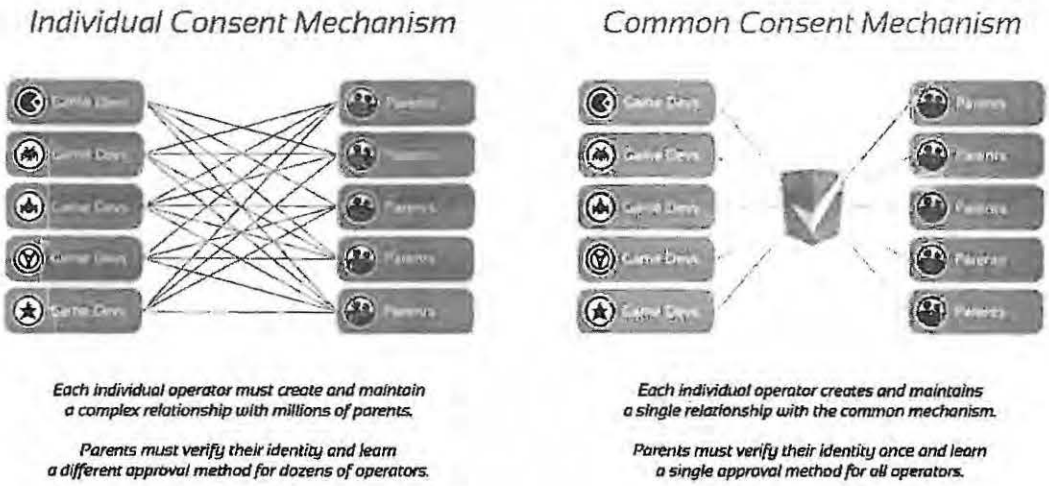
This application therefore proposes an unenumerated method for (i) associating a verified parental identity, (ii) obtaining parental approval, and (iii) (if not approved) blocking the app on the smartphone or tablet (or website) in use by the child. We propose—and have developed—a device-based, real-time, platform-based method to associate parental identity with the device and a specific app, which achieves the Commission's vision of a reliable, manageable, parent-curated online experience for children using smartphones, tablets, or PCs who interact with mobile applications or other online services. See Figure 1, below.

26 *Id.*

27 *Id.*

28 *Id.* at 3,990. When discussing "common consent mechanisms," the notice accompanying the Final Rule mistakenly refers at page 3,990 to "Section 312.5(3)", which does not exist. Given the inclusion of the phrase "voluntary Commission approval process," discussed at length on page 3,991, we have interpreted this language to be referring to 16 C.F.R. § 312.12, Voluntary Commission Approval Processes, under which AgeCheq seeks Commission approval of a parental consent method not currently enumerated in § 312.5(b). Section 312.5(b)(3) deals with the ability of already approved safe harbors to approve not currently enumerated methods.

Figure 1 - Benefits of a Common Consent Mechanism



In view of the challenges inherent in verifying parental consent for children to use individual apps, the method described herein provides a new, unique method for verifying parental consent, namely linking a verified parental identity to a specific device associated with a child, and permitting the parent to curate the child's access to unlimited numbers of apps via a common mechanism, on a real-time, automated basis. This real-time, device-based, common consent management system ("Real-Time Common Consent Mechanism," or "RCCM") allows parents to complete a single, COPPA-compliant verification process, which may then be overlaid across apps produced by participating developers. The RCCM materially extends currently enumerated verification methods (credit card, faxed/emailed form, for example) by adding real-time, hubbed parental identification, notice, and consent management for multiple apps and devices (desktop, tablet, and smartphone), as depicted in Figure 2, below.

Figure 2 – System Architecture – Hubbed Parental Identification, Notice, and Consent

REDACTED

Under the proposed RCCM, this verified identity is linked to a secure parent account, which in turn is linked to device(s) used by the parent's child/ren. As the Commission has recognized, the unique identifiers associated with a device can be used to track its use across online services.[29] In addition, a dashboard allows parents to temporarily block the child from running one or more previously approved apps, or to permanently revoke their permission for the child to use the app. As required by the Rule, when a parent permanently revokes permission, the RCCM notifies the app's publisher and also any third party ad networks that parental revocation has been made. Following notification, it is the responsibility of the developer and third parties to delete the personal information they captured as required by the Rule.

Under the method we are proposing, app developers and parents independently register with the common consent mechanism administrator, for example, AgeCheq. The parent

29 *See* 76 Fed. Reg. 59,812 (2011).

undergoes an identity verification step, and registers the child's device. The smartphone or tablet is associated with the parent's (AgeCheq) account through real-time automated communication between the RCCM servers and the mobile device. Developers also interact directly with the common platform, by registering and uploading information about their information collection, use and sharing practices, including a link to the full privacy policy. The developer integrates RCCM validation checking code into their application. Ad networks may also be registered. When a child attempts to download or access a (registered) app from a (registered) device, the parent will receive layered and comprehensive COPPA disclosures.

By linking parents, devices, and developers in this manner on a shared (AgeCheq) platform, parents can thereafter affirmatively grant authorization for the child to use the app (or revoke permissions at any time). Fundamentally, apps are blocked from use until a parent has (a) received a notification including COPPA notices from the developer, and (b) personally enabled access, which is then (c) accomplished in real time when the app receives a positive validation response from the RCCM. Developers are responsible for incorporating the RCCM into their app and ensuring that approval or rejection responses received from the RCCM are responded to appropriately (by unlocking the app or leaving it blocked).

Moreover, when each registered/authorized app starts-up, the RCCM validation checking code seeks confirmation from RCCM servers that the device has been authorized to use the app. This ensures that not only may parents initially grant approval, but that they may later retract that approval and return the app to its locked state. If the RCCM code determines that the app is not authorized, the app alerts the child that parental permission is required, prompting the parent to either login to their existing RCCM account, or create and verify a new account. The RCCM

could also integrate other notification options, such as parental alerts via email or SMS text message.

In keeping with its "real time" approach, the RCCM delivers "just-in-time" privacy disclosures.[30] Developers who use the method must complete a privacy disclosure survey, which is stored in the RCCM database, along with the privacy disclosures of any third-party ad networks used in the app. Per the Rule, when the parent is using the parental dashboard to approve an app that the child wants to use, the parent must first view a privacy disclosure screen that denotes all personal information captured by the app and by its third party component application programming interfaces ("APIs"). The RCCM offers parents many different ways to view this privacy disclosure, but at all times, the developer's full-text privacy policy is available with a single click.[31]

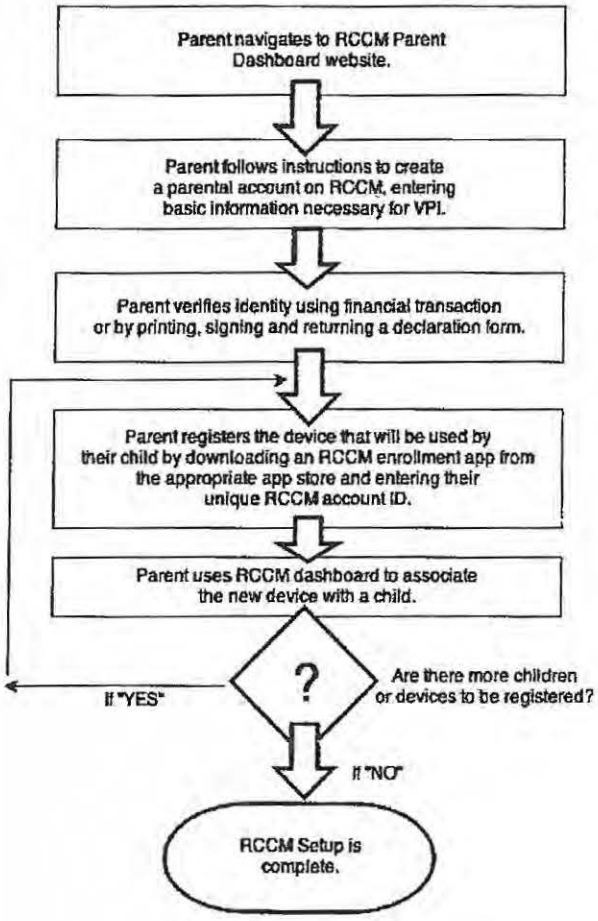
Importantly, the proposed method is not merely feasible—it is available today. AgeCheq has fully built and operates a RCCM using the proposed method. Accompanying this application, as a proof of concept for the proposed RCCM, are narrated video and pictorial representations of the proposed RCCM as implemented by AgeCheq. Obviously, the Commission is not charged with approving or disapproving particular companies' or organizations' business plans or methods. Rather, the purpose of the AgeCheq materials attached to this application is to demonstrate the feasibility of a common consent mechanism based on real-time, device-based methods for verifying that an identified parent has authorized

30 *See, e.g., Mobile Privacy Disclosures: Building Trust Through Transparency*, FTC Staff Report (Feb. 2013), at ii, *available at* http://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission (stating that "app developers should ... Provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information (to the extent the platforms have not already provided such disclosures and obtained such consent)").

31 *See* Computer and Communications Industry Association ("CCIA") (comment 27, 2011 NPRM), at 7.

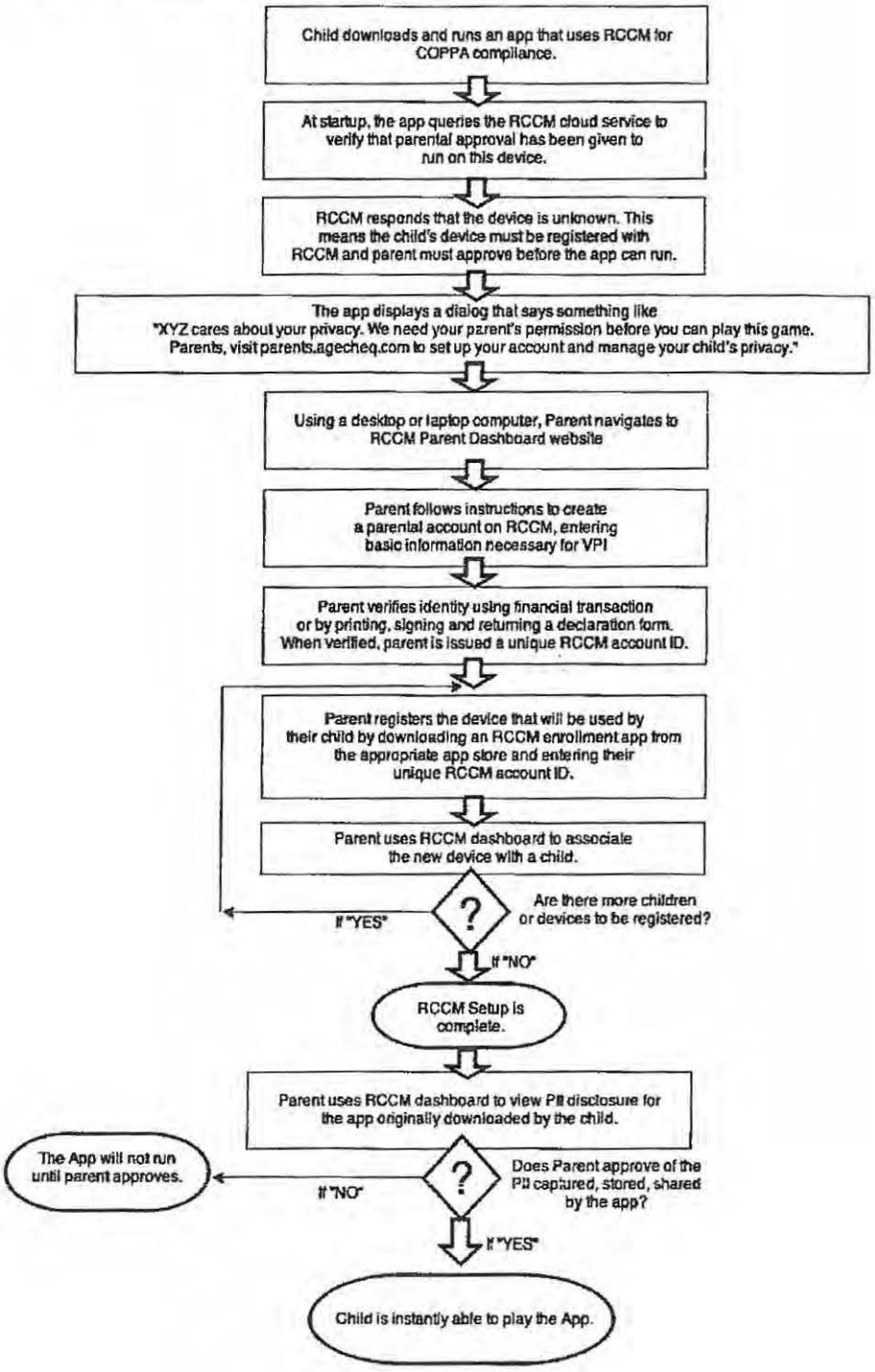
the collection of information from or about an identified (child's) device via an identified app. Figures 3, 4, and 5, below (along with their accompanying online videos) depict the proposed method, which can be replicated by other providers or platforms. Specifically, Figure 3 depicts how a parent can proactively create and verify an RCCM account, Figure 4 depicts how a parent can create and verify an RCCM account in response to their child being unable to access a desired app, and Figure 5 depicts the typical scenario for providing notice and obtaining consent from a verified parent with a preexisting RCCM account.

Figure 3 – Proactive Initial RCCM Account Creation Flow[32]



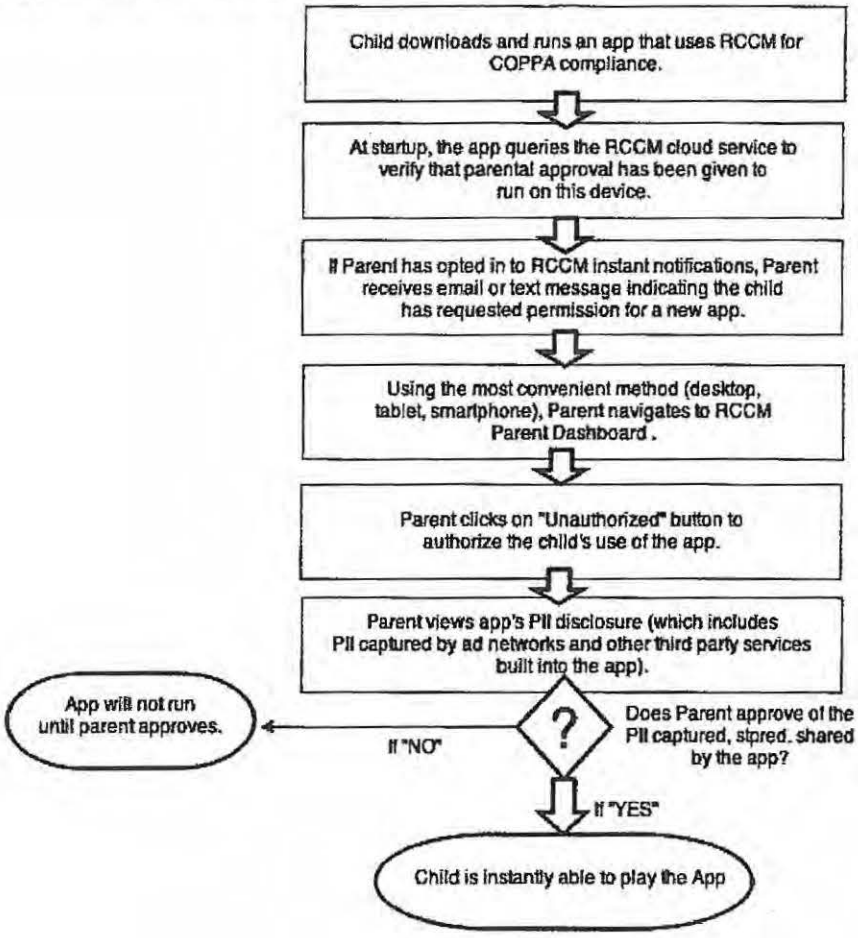
32 For a video demonstration of this process, please visit: http://vimeo.com/agecheq/review/101104468/7e7ae4941c.

Figure 4 - Reactive Initial RCCM Account Creation Flow[33]



33 For a video demonstration of this process, please visit: http://vimeo.com/agecheq/review/101104516/935919e707.

Figure 5 - Typical RCCM Parental App Approval Flow[34]



CONCLUSION

The Children's Online Privacy Protection Act and its implementing Rule are, at present, weakly applied to the mobile ecosystem. Many apps are created by small developers with few resources for the costly and complicated parental verification and consent process.[35] The Commission has suggested that a third-party might create this process on behalf of app

34 For a video demonstration of this process, please visit: http://vimeo.com/agecheq/review/101104651/44bb720002.

35 *See* Connect Safely (comment 21, 2012 SNPRM), at 3.

developers,[36] but has yet to approve any such common consent mechanisms, leaving the industry hesitant to transition to third-party COPPA compliance platforms.[37] With this application, the Commission has the opportunity to approve a unique new method for verifying—in real-time—that a properly identified parent has authorized a particular device to download or use a particular app. 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. By approving this method, the Commission can enable developers to comply with the COPPA rule and empower parents to make informed decisions about their children's online privacy. The RCCM could even promote the creation of innovative new apps for young children. Freed from the costly burden of one-off, app-by-app, verifications and notifications, both parental engagement and developer compliance would be expected to improve.[38]

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 real-time common consent mechanism.

Sincerely,

Roy R. Smith II, CEO

36 *See supra* n. 5.

37 *See* 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 (in fact, the Commission has expressly rejected past applications to approve common consent mechanisms).

38 *See* CCIA, at 8.