

Privacy Vaults Online, Inc. d/b/a/ PRIVO, an authorized Safe Harbor provider under the Children's Online Privacy Protection Act ("COPPA") hereby responds to the Commission's "Questions on the Parental Consent Method" it has published in connection with the application for approval of parental verification method filed by AgeCheq Inc. on July 25, 2014.

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 Section 312.5(b)(1) of the Rule?

PRIVO submits that AgeCheq's filing at the FTC is not an application for approval of a new parental consent mechanism, but is in fact a business plan for a parental consent management intermediary, which the FTC has previously termed an "infomediary." The FTC has long encouraged the development of such intermediary services, which it defined at least as early as 2005 as services that "act as middlemen in obtaining verifiable parental consent for Web sites and can offer options such as driver's license and social security number verification."¹ In 2005, the FTC undertook a review of its COPPA Rule, 16 C.F.R. §312.1 *et seq.*, in large part to determine whether to retain the Email Plus method of parent verification.² In connection with that review, the FTC asked for comments on the availability and development of "infomediary" services. It noted that only one such service identified itself, and that service was PRIVO, which, the FTC noted, had been approved as a Safe Harbor in 2004.³ The FTC concluded that such services were not at that time abundantly available and that it should retain the Email Plus

¹ *Children's Online Privacy Protection Rule*, 71 Fed. Reg. 13247, 13256 (March 15, 2006).

² *Children's Online Privacy Protection Rule*, 70 Fed. Reg. 21107 (April 22, 2005).

³ *Children's Online Privacy Protection Rule*, 71 Fed. Reg. 13247, 13256 (March 15, 2006).

method of parental verification for some uses, because it was broadly available and readily implemented by businesses.⁴

The FTC has now received multiple applications under Section 312.12 in which the proponent describes a centralized database, known in privacy circles as a Consent Management Authority (“CMA”), which is intended to reduce the need for parents to re-verify themselves to multiple online services.⁵ There may be great public benefit to the existence and use of various intermediary services, but, as PRIVO has previously said in each such case, this concept is not new. Indeed, PRIVO’s 2004 Safe Harbor application included a youth registration and parental consent management service that included registration, authentication, authorization, ID vetting and account management of personal information and the parental consent associated with it, on a service by service basis. Moreover, it is not a *method*.⁶ Rather, these are different examples of implementations of the already approved methods of parental verification under COPPA.

The AgeCheq application is instructive in this regard. AgeCheq describes itself as allowing “a parent to curate a child’s mobile application (“app”) experience in real-time, through automated, device-level, **implementation** of verified parental consent.”⁷ Later, AgeCheq acknowledges that “[t]he proposed method incorporates, but uniquely extends, tried and true (legacy) methods to verify parental identity . . .”⁸ AgeCheq uses three already approved methods. First, in establishing the parent account, AgeCheq collects the parent’s first and last

⁴ *Id.*

⁵ See AssertId FTC Matter No. P135415; Imperium FTC Matter No. P135419; iVeriFly FTC Matter No. P135420.

⁶ In the alternative, if the FTC were to decide that parental consent intermediary services are a method, than it has already approved of them, but only with the additional safeguards and obligations of an approved Safe Harbor, as is the case with PRIVO.

⁷ Letter to Donald S. Clark, Secretary from Roy R. Smith, II (July 25, 2014) at 1.

⁸ *Id.* at 1-2.

name, address, and last four digits of Social Security Number,⁹ an already approved method. Once the account is established, AgeCheq again verifies parental consent through one of two existing methods. The free method of verification uses a print and send form, and the paid method of verification requires a \$4.99 charge on the parent's credit card.¹⁰ As the FTC most recently said in response to the iVeriFly application,¹¹ a cobbling together of various approved methods does not constitute a unique new method.

AgeCheq does add the element of collecting the device ID of the device that the parent asserts is the child's device. While this information collection can alleviate the need to implement usernames and passwords that are disruptive to the mobile user experience, the process of binding a unique identifier to an account is nothing new. It is essentially the mobile equivalent of the "Remember Me" box seen on many websites or a cookie on a browser. In fact, all compliant services have to do this in one form or another to allow the service to be able to fulfill the request of a parent to stop collecting and/or to delete child data. Thus, while the AgeCheq application may present an implementation of the approved verification methods that the FTC has not previously included in Section 312.5(b)(1), that is not a reason to add it to the list. In fact, it is appropriate that the FTC has not listed binding a unique identifier to an account to its list.

First, the mere fact of binding has nothing to do with verification. The verification has to occur before the binding is of any use. Second, there are many different unique identifiers that

⁹ See How AgeCheq-Enabled Apps and the Parent Dashboard Interact available at <http://vimeo.com/99654950> (last visited September 30, 2014).

¹⁰ *Id.*

¹¹ iVeriFly FTC Matter No. P135420.

could be bound. Some present more privacy risks, for example, full, unencrypted Social Security Numbers, while others might be less useful in establishing identity, such as shoe size. The FTC would have to delineate specifically which unique identifiers would be acceptable and which would not. Further, that list might change over time with technological developments, requiring the FTC to continually update the list.

Finally, the FTC's processes should not be used to approve the specific business plan or proprietary products of specific companies. Doing so could lead to confusion among developers that they must use a service or product that is listed in the FTC's rules or they will be at risk of noncompliance. Indeed, AgeCheq has said publicly that "[t]he safe harbor nod is 'really not the kind of iron-clad guaranteed approval that the people we are selling to want.'"¹² As a result, to satisfy app developers, AgeCheq apparently feels that it will not benefit from the assistance of a Safe Harbor, but must "get our entire system explicitly approved by the FTC."¹³ Thus, it is clear that, if approved, the AgeCheq infomediary service will be seen in the marketplace as providing full COPPA compliance in and of itself, which it does not, and that using any other company's implementation, though offering similar features, might be risky.¹⁴ Moreover, the FTC was

¹² *With Widespread COPPA Noncompliance, FTC Enforcement Action Seen*, Communications Daily, August 28, 2014 at 8.

¹³ *Id.*

¹⁴ Website operators and mobile app developers are primarily focused on producing a quality product that provides a positive user experience, and are desperately seeking any authoritative statement that they are "COPPA-compliant." As a result, they are susceptible to the impression left in the marketplace by the FTC parent verification method approval process. Thus, while PRIVO agreed that the Knowledge Based Authentication was appropriately added to the FTC's list, reporting on the FTC's approval of that method implicitly, and in some cases explicitly, stated that the approval was tied to the applicant's particular implementation of the method. Consider the following from BloombergBNA which was published a week after the Commission's decision, when there had been a considerable opportunity to have carefully analyzed the decision before publishing news concerning it:

FTC Gives Stamp of Approval to COPPA Parental Consent Method by Imperium

clearly looking to the marketplace to answer the call for infomediary services on its own. It did not intend to give individual companies a PR boost through this process. Yet, even with the denial of an application, this can be what happens. Articles such as the one quoted above are published when the application is filed and no determination has been made as to its validity, but the mere fact that the applicant has voluntarily agreed to undergo a government review nonetheless provides it with an air of legitimacy. A denial letter, if it is worded to allow the

Monday, December 30, 2013

The Federal Trade Commission Dec. 23 announced that it had approved a verifiable parental consent method under the Children's Online Privacy Protection Rule proposed by Imperium LLC.

The FTC's approval of the consent method proposed by Westport, Conn.-based Imperium follows the commission's rejection in November 2013 of a separate consent method proposed by AssertID Inc. (221 PRA, 11/15/13).

The commission had said AssertID's proposed method did not meet the approval criteria in the COPPA Rule, which implements the Children's Online Privacy Protection Act. AssertID's consent method was based on peer verifications through a parent's social network.

In its latest action, the FTC approved Imperium's proposed use of "knowledge-based authentication" (KBA), which verifies a user's identity "by asking a series of challenge questions," according to a Dec. 23 statement by the FTC.¹⁴

<http://www.bna.com/ftc-gives-stamp-n17179881019/>. Almost no amount of further explanation following those opening paragraphs could possibly adequately convey to the reader that the Commission's approval was not inextricably tied to the implementation of KBA presented by Imperium or undo the impression left by numerous news articles that were published before it.

For example, DataGuidance reported: The FTC approved the application submitted by Imperium, Inc. which provided for a knowledge-based identification (KBA) process as it "offers the individual an opportunity to be verified by answering challenging questions [...] which are difficult for someone other than the individual to answer." . . . As the method has now been approved other businesses are now also entitled to implement it as an acceptable form of obtaining parental consent. Imperium founder and CEO Marshall Harrison said, "We are gratified to be the only new method approved by the FTC for Verified Parental Consent for COPPA. We look forward to working with the industry to protect children from unsafe practices." See <http://dataguidance.com/news.asp?id=2183>. The quoted language is used in a confusing manner and reasonably leads to an impression that the "it" that was approved was only Imperium's implementation of KBA, rather than KBA more generally.

In another example, PR Newswire carried this: Imperium®, an established industry leader in fraud prevention and identity validation solutions, is pleased to announce that ChildGuardOnline has received approval from the FTC for its knowledge-based authentication method used to obtain verifiable parental consent. This approval signifies that online businesses that request information from children under the age of 13 now have a new, more technologically-advanced option to comply with COPPA. <http://www.prnewswire.com/news-releases/ftc-approves-childguardonlines-new-method-for-parental-consent-verification-239462071.html>.

applicant to later assert that the FTC had ruled that its implementation, while perhaps not unique, was at least COPPA-compliant, can also be a marketing asset to the applicant. As PRIVO has said before, approving, and even entertaining, applications for “new” verification methods that do not present anything new, risks an arms race among existing and would-be infomediaries, as each feels it must legitimize its business plan by going through the FTC process.

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.

As stated, the AgeCheq application does not present a new methodology to be considered under this standard. AgeCheq’s application is primarily about providing a Consent Management Authority. The only CMA that the FTC has ever approved is PRIVO, and then only as part of an approved Safe Harbor. PRIVO submits that this is the only appropriate way for the FTC to do so.¹⁵ As a Safe Harbor, PRIVO is subject to the FTC’s on-going review. In contrast, something approved through the Section 312.12 process is not subject to any such further review. Thus, changes in the company’s business practices could go unnoticed and without any vetting as to their impact on COPPA compliance.

Moreover, being a central repository of identity information is an immense undertaking. The identity ecosystem is currently undergoing a huge evolution driving towards privacy enhancing, interoperable, easy to use, cost-effective, secure and resilient identity credentials

¹⁵ In the alternative, a proposed infomediary could work with a Safe Harbor to help assure that its practices are compliant at the outset and remain compliant and represent best practices in the privacy industry despite the passage of time or changes in technology.

governed by auditable identity trust frameworks defining legal, technical, and operational policies that must be followed by all participants. The U.S. Government, through its National Strategy for Trusted Identities in Cyberspace, the National Institutes for Standards in Technology, and the Department of Commerce, working together with industry stakeholders, other agencies, and international entities is developing standards that should apply to any organization holding, or enabling the release of, such sensitive data. If a Consent Management Authority is approved through the Section 312.12 process, it will have secured a significant government benefit without any concomitant obligation to adhere to the standards adopted across the government.

Moreover, the AgeCheq service does not appear to meet all the requirements of COPPA. For example, the language in its default age-gate would likely be very alarming to a child user and lead the child to lie about its age to be able to use the app.¹⁶ In addition, the parent dashboard presents an “all or nothing” option to consent. The parent cannot exercise any choice and must allow all data collections proposed by the app or deny all such collections.¹⁷ Although PRIVO does not doubt that appropriate compliance remediation could be made, the mere use of the service does not make its customers COPPA-compliant.

3. Does this proposed method pose a risk to consumers’ personal information? If so, is that risk outweighed by the benefit to consumers and businesses of using this method?

It is noted that a parental consent management intermediary service itself triggers COPPA. AgeCheq itself will be able to track users’ actions across online services and over time

¹⁶ See Using An Age Gate With the AgeCheq Unity SDK available at <http://vimeo.com/99654950> (last visited September 30, 2014).

¹⁷ See How AgeCheq-Enabled Apps and the Parent Dashboard Interact available at <http://vimeo.com/99654950> (last visited September 30, 2014).

