

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 second application for approval of parental verification method filed by AgeCheq Inc. on October 1, 2014 (the "Second Application").

Stripped to its essence, the Second Application asks whether sending a verification code via text to a self-asserted cell phone number and requiring that the verification code be entered on an otherwise unverified and unverifiable digitally signed certification form adds sufficient indicia of reliability such that online services can rely on that digital signature for the full panoply of uses, including third-party sharing and public disclosure. If the answer to this first question is affirmative, the Second Application asks whether a third party can handle sending the text messages and receiving the digitally signed forms for operators so that they do not have to.

PRIVO submits that, at best, adding a verification code sent via a self-asserted cell phone number to a form that is signed digitally might provide a level of reliability equivalent to that of the Email Plus method in some circumstances. However, the method can never be used on a child-directed site because the operator cannot collect a parent cell phone number directly from a child and the operator cannot instruct the child to ask the parent to supply the cell phone number or register at a third party site, i.e., the Parent With Me approach.¹ Therefore, those operators using the proposed method would nevertheless have to collect a parent email or other online

¹ The COPPA Rule specifically provides that on a child directed site, the only information that would not be considered personal information and can be collected directly on the site is parent online contact information, traditionally, an email address. In this regard, it is noted that increasingly, children do not have email addresses but rather use text and social media to communicate. As a result, the Email Plus method of parental verification is likely stronger today than when it was initially adopted.

identifier and secure the cell phone number from the parent, which is the Email Plus method. Where the method could perhaps stand on its own, without collecting a parent email or other online identifier, would be on a general audience or mixed audience site or service that uses an age-gate, because the operator can collect the cell phone number from those users who identify themselves as being over the age of 12. However, that consent may only be relied upon for internal uses, not for online sharing or public disclosure such as picture or video upload or online communication in the absence of pre-moderation. To date, the safe harbors, informed by discussions with Commission staff, have required email verification for the Parent With Me approach, that is where the holder of a self-asserted parent account wants to add a login credential for a child sub-account. Underlying this approach is the understanding that the operator cannot assume that the parent is with the child, i.e., the one providing the child's information, and that once children can provide data directly to the service, all data in the profile record is subject to COPPA and the requirement that operators collect a parent online identifier to deliver notice and request consent or otherwise verify the identity at a more reliable level in conjunction with delivery of the online privacy notice.

Given the complexities of when this method would be appropriate, there is substantial risk that operators will use it inappropriately, especially if it is marketed as a third-party solution for COPPA compliance and hailed as superior to existing methods for permitting the full panoply of COPPA-triggering activities, including public disclosure and third party sharing.

Finally, PRIVO notes that the Commission has long sought alternatives to the Email Plus method of verification. Therefore, approving another method for mass use in the industry that

provides only an equivalent amount of reliability would be a retreat from the Commission's long-standing goal of moving to more reliable methods.

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?

At first blush, the Second Application appears to propose using the "sign and send" method of verification which has long been one of the enumerated methods of verification contained in Section 312.5(b) of the Rule. Because the sign and send method is already enumerated, that aspect of the Second Application is not new. However, the way AgeCheq proposes implementing this established method makes it less reliable because it makes it easy for children to do on their own and reduces all handwritten material on the form, from the manual signature itself to an accompanying printed name, signature date, address, or phone number, which undermines the ability to assess whether the handwriting is that of a child or of an adult.

This is because the Second Application proposes that the signature on the form will be provided digitally, on screen, with a stylus, finger or mouse.² The Commission has previously ruled that an on-screen digital signature alone is not sufficiently reliable for purposes of the Rule.³ To work around the Commission's position on this matter, the Second Application

² Letter to Donald S. Clark, Secretary from Roy R. Smith, II (October 1, 2014) at 4 [*hereinafter* "Second Application"].

³ *Children's Online Privacy Protection Rule*, 78 Fed. Reg. 3971, 3988 (January 17, 2013).

proposes to also collect a self-asserted cell phone number, send a verification code to that cell phone number, and require that the verification code be entered on the digitally signed form.⁴

However, collecting a cell phone number and requiring an account holder to enter a verification code sent to that cell phone number is nothing new to operators of general audience and mixed audience sites and services. These operators routinely use an age-gate and begin communicating directly with those users who indicate that they are over the age of 12. In this scenario, they can request any personal information, including cell phone number, as part of the registration process. As stated previously, though, once data is collected about a child, such as where the parent creates a child account to permit the child to access the site or service, the operator must follow the Parent With Me approach and undertake further verification of the purported adult attribute. The type of further verification required at this stage depends on whether the operator seeks consent to use that child data only for internal operations or for sharing/public disclosure activities. This process is standard in the industry by now and certainly nothing new.

What could be considered a "new" approach is that the Second Application seeks to skip this further verification of the purported adult, and it seeks to do so on both child-directed and general/mixed audience sites and for both internal uses and third party sharing/public disclosure. Had the Second Application proposed some sort of additional account verification, PRIVO would simply state that the text verification code process is not new and does not require Commission approval. However, because there appears to be no additional verification, as explained in the next section, PRIVO submits that the proposed parental consent method is **not**

⁴ *Second Application* at 3.

reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. And, as AgeCheq acknowledges, the Commission has already rejected this approach.⁵

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.

The purported innovation for which the Second Application seeks approval is the sending of a verification code to a self-asserted cell phone number. As PRIVO explained in its Comments to the first AgeCheq application, the use of a verification code (or a password or response to a challenge question) has nothing to do with verification of the accountholder information in the first instance. That verification has to occur before a correct response with a verification code (or password or challenge question answer) can provide the level of reliability AgeCheq seeks.

Nevertheless, AgeCheq claims that even without such verification its method is reliable because the parental datapoints to be collected – name, address, birth year and cell phone number – are not entered on the operator's screen where the child is attempting to register, but are

⁵ It is worth noting that AgeCheq repeatedly states that digital signatures are not an acceptable method of parental consent verification. That is not the case. Digital signatures can be acceptable when accompanied by appropriate additional verification of identity. Unfortunately, what AgeCheq is proposing does not provide the type of verification needed for reliance on a digital signature.

entered at a third-party website that children are unlikely to visit.⁶ This is essentially the reasoning behind the Email Plus method as well. That is, it is considered unlikely that children will take all the steps necessary to set up a false email account, enter that email address when prompted by an online service to provide a parent email, log into the false account, respond to the first email from the operator and then log into the false account a second time and respond to a second, confirming, email. Therefore, to the extent that the basis of AgeCheq's claim of reliability is that the entry of the parent's email at a child-directed site or service and the signing of the consent form at a third party's site are separated in time and space, then it is no different than Email Plus. It is simply another step, a different Plus, in Email Plus. However, AgeCheq itself notes that the operator could implement the method directly on its site, in which case, there would be no such separation in time and space.⁷ Either way, it is likely even less work for a child to circumvent this method than the Email Plus method.

This is because AgeCheq proposes to rely on the fact that the mobile phone a child uses to access an operator's service is provided to the child by an adult who pays for the phone, has authority over the phone, and presumably can access or control access to the phone.⁸ However, under the COPPA Rule, on a child-directed site or service, the operator is required to assume that all users are under the age of 13 at the outset and cannot rely on the likelihood that a parent is in the vicinity of the desktop computer when the child is using it or has control of the mobile device when the child is using it -- the Parent With Me approach.

⁶ *Second Application* at 6.

⁷ *Id.* at 2, n 4.

⁸ *Id.* at 7-8.

Moreover, this potential *de jure* access to the device cannot be relied upon given the widespread practice of parents handing the parent's phone to a child to play with while the parent is otherwise engaged. In that scenario, even if the parent previously completed the initial registration at the third party's registration page, the child will be in possession of the very device that the process is initiated from and is to receive the verification. Unlike other verification methods such as email, PayPal or social media accounts which parents are likely to close when handing the device to a child, texting is likely not access-controlled leaving it open to the child's use. While the text may appear on the parent's device for the parent to discover later, the text is easily erased. Even where the parent has provided the child with a separate device, it is unlikely that the parent is regularly reviewing the texts received on that device to determine whether any verification codes for COPPA compliance have been received on it. Moreover, the parent's "power of the pocketbook" cannot be relied on the way it is in the case of the credit card method of verification. The parent simply does not receive the sort of itemized bill showing the receipt of a parental verification code text message by the child's device equivalent to what he or she would receive when their credit card has been charged in connection with giving consent under COPPA. Therefore, the parent's payment of the phone bill does not serve to alert the parent to any potential subterfuge by the child. If the carriers would provide assistance in the verification process on behalf of their customers, they could verify unique data and provide notice on billing statements.

As a result, whether the child is using the parent's device or a separate one provided by the parent, it is highly likely that the child will receive the verification code and be able to enter it on the form and sign the form him or herself. In the offline version of the "sign and send"

method, the signed form is actually received and reviewed by a responsible party, such as the operator or PRIVO. In PRIVO's experience, it is often very easy to identify forms which are likely to have been signed by a child and to take follow-up steps to verify those signatures. This is particularly true given that only a small proportion of parents choose the print and send option, thereby reducing the number of forms and making the process of reviewing them practical. In the case of the method proposed in the Second Application, on-screen signing appears to result in a frequently childish-looking signature, making any effort to distinguish child-signed forms from adult-signed forms futile. In fact, AgeCheq does not state that any such review is a part of the proposed method. At most, the ability to save files and later review them is an option the method leaves open for each third-party intermediary to pursue or not as it pleases.⁹

Therefore, if this method is ever to be considered more reliable than Email Plus, verification of the self-asserted parental datapoints in excess of what AgeCheq has proposed must take place before the verification code methodology is implemented. Examples of the type of verification that might be sufficient include: Verifying with the cellular provider that the self-asserted cell phone number is that of the primary accountholder and requesting that the cellular provider deliver the privacy notice, request for verifiable consent, and verification code to the accountholder's online identifier of record; or verifying the self-asserted account information along with a unique identifier or Knowledge Based Authentication questions that only an adult should be able to respond to against traditional sources such as credit bureaus. In PRIVO's experience, the carriers have been reluctant to provide information such as the age of the users of each device that would be necessary for the first example to work. The traditional methods

⁹ *Id* at 8.

referred to in the second example are those that have already been approved by the Commission, and thus would not need any additional approval.

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 not clear from the Second Application what the universe of information to be collected from parents is and what types of information storage and security practices are to be implemented. For example, AgeCheq states that different third party intermediaries can make different choices as to what information to collect in the first instance and what of it to retain.¹⁰ In fact, it is not even clear from the Second Application whether the information retention practices AgeCheq would engage in or expects the Commission to mandate for operators other third party intermediaries will comply with other requirements of COPPA. Specifically, AgeCheq states that the third party intermediary will know that someone from a specified cell phone number digitally signed the consent form, using a matching verification code, on a certain date at a certain time.¹¹ It is not clear from this description, though, how the operator will be able to respond to a demand by a purported parent that the operator provide the purported parent with access to the data it has collected from a specified child and/or that the operator stop collecting or delete that data. At a minimum, it is likely that a handwriting comparison between a manual signature and the digital signature that the intermediary might optionally retain will be of limited value given that the digital signature process may distort the signature to some extent.

¹⁰ *Id.*

¹¹ *Id.*

Due to the uncertainty regarding whether the proposed process will provide operators with the information they need to comply with all aspects of the COPPA Rule, and the apparent lack of independent verification of the self-asserted parental data and resulting Email Plus-only level of reliability appropriate for limited uses that the method will provide, PRIVO submits that any risk to consumers' information is not outweighed by the meager benefits the proposed method appears to confer.

Conclusion

PRIVO submits that AgeCheq's Second Application suffers from the same misunderstanding of the Commission's rules and parental consent mechanism approval process as AgeCheq's first application, which the Commission has turned down as unnecessary. Specifically, much of the Second Application does not propose a new consent mechanism so much as sets out a business plan for a parental consent management intermediary of the type that the FTC has termed an "infomediary." The FTC has long encouraged the development of such intermediary services, which it defines 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."¹² In 2005, the Commission noted that only PRIVO, whose 2004 Safe Harbor application included a youth registration and parental consent management service encompassing registration, authentication, authorization, ID vetting and account management of personal information and the parental consent associated with it, was the only infomediary with

¹² *Children's Online Privacy Protection Rule*, 71 Fed. Reg. 13247, 13256 (March 15, 2006).

