CENTER FOR DEMOCRACY & TECHNOLOGY

August 21, 2023

To: Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW, Suite CC–5610 (Annex P)
Washington, DC 20580

Re: Application for Parental Consent Method, Project No. P235402

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the Federal Trade Commission's (FTC) request for comment regarding the Entertainment Software Rating Board, Yoti, and SuperAwesome's ("the ESRB group") proposed parental consent method. CDT neither supports nor opposes the ESRB group's proposal.

We write because the question of what constitutes adequate assurance that a person acting on behalf of a child is a parent has increasingly broad implications beyond the Children's Online Privacy Protection Act (COPPA). Both federal and state bills increasingly contain provisions that explicitly or implicitly require determining the existence of a parent-child relationship.[1] The Commission's guidance on what is a sufficiently reliable indicator of such a relationship will have significant influence in these settings in addition to COPPA.

The ESRB group proposal raises that question in stark form: whether evidence that a person is older than 25, standing alone, is sufficient to reasonably ensure that the person is a parent of a child who provided that person's email address as belonging to their parent. In answering that question, the Commission should keep in mind the broader ramifications that its decision and rationale could have for the online ecosystem.

[1] *See, e.g.,* Protecting Kids on Social Media Act (Apr. 26, 2023) (requiring parental consent, "taking into account current parent or guardian relationship verification technologies and documentation," before minors between the ages of 13 and 18 can establish social media account), https://www.schatz.senate.gov/imo/media/doc/protecting_kids_on_social_media_act_2023.pdf; Kids Online Safety Act (July 27, 2023) (requiring that "parents" be permitted to view and change a child's privacy and account settings), https://www.congress.gov/bill/118th-congress/senate-bill/1409/text#toc-id835701d0-c064-42db-b2af-8eb6591ac0e1.

CENTER FOR DEMOCRACY & TECHNOLOGY

I. Does the proposed method provide sufficient indicia that the person consenting is the child's parent? *(Questions 1 and 2)*

The standard under 16 CFR 312.5(b)(1) for allowing a new method to obtain verifiable parental consent is that the method "must be reasonably calculated, in light of any available technology, to ensure that the person providing consent is the child's parent." The ESRB proposal is designed to confirm that the person providing consent is older than 25, which the proposal asserts means they are "old enough to be a parent."[2] Anyone whose email address a child provides and whom the system estimates is older than 25 can provide consent for the child. According to the applicants, "[a]ll the currently approved VPC methods establish that the person is an adult; none of them definitively authenticates the parent-child relationship."[3] The question the FTC must answer is whether a facial estimate that someone is older than 25, standing alone, is sufficient to meet the applicable standard.

A. Verifiable parental consent methods the Commission previously approved combine multiple indicators of reliability.

Generally, verifiable parental consent mechanisms require multiple indicators of reliability to ensure the person consenting is the child's parent. While the applicants rightly note that prior-approved methods do not definitively ensure that the person consenting is in fact the child's parent, those methods include enough friction to at least make it less likely that the person is not the child's parent.

For example, Riyo's proposed method approved by the FTC involves a multi-step process. Riyo's method required first providing an image of a government-issued photo identification that is authenticated via software that uses computer vision, algorithms, and image forensics to analyze information on the photo identification as well as fonts, holograms, and other features of the photo identification.[4] Then, facial matching is used with liveness detection to verify that

[2] Entertainment Safety Ratings Board, Application for Approval of a Verifiable Parental Consent Method Pursuant to the Children's Online Privacy Protection Rule 16 CFR 312.12(a) (June 2, 2023), at 8, https://www.ftc.gov/system/files/ftc_gov/pdf/Application-for-a-new-VPC-method-ESRB-SuperAwesome-Yoti-06-02-2023.pdf [hereinafter "ESRB Group Application"].
[3] *Id.* at 9.
[4] Federal Trade Commission, Letter Re: Jest8 Limited's (Trading as Riyo) Application for Approval of a Verifiable Parental Consent Method (2015), https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf.

the person providing consent is the person to whom the authenticated photo identification was issued.

Imperium similarly proposed a multi-step process to ascertain the consenting person's relationship to the child and confirm the person's identity. The consenting person provides their name, address, and age, and Imperium confirms the consenting person and child's address is the same, that the consenting person's age is at least sixteen years older than the child's age, and the identity of the consenting person. If the identity cannot be successfully verified via the last four digits of the consenting person's Social Security Number, Imperium then uses knowledge-based authentication. The Commission's approval of Imperium's proposal stated that "entities handling sensitive information, including financial institutions and credit bureaus, have used [knowledge-based authentication] to authenticate users for many years."[5] The Commission determined that evidence shows this method is "sufficiently reliable to verify that individuals are parents authorized to consent to the collection of children's personal information," as long as (1) the method includes a reasonable number of challenge questions with an adequate number of possible answers so that the probability of simply guessing the correct answers is low, and (2) the questions are sufficiently difficult so that a child age twelve or under in the parent's household could not reasonably ascertain the answers.

In both cases, the verification method seeks to confirm both the consenting person's age and their identity – through facial matching with a government-issued ID in the case of Riyo and through either a partial SSN or knowledge-based authentication in the case of Imperium. The ESRB group points to Riyo's method as closest to its own, but agrees it is distinct. As the ESRB group notes, their proposed method "is not used to determine that the individual is who they claim to be, but to determine that the individual is the *age* they claim to be."[6]

Further, the ESRB group's proposal includes almost no friction and is designed to be "an easy way to provide [verifiable parental consent] through a quick process."[7] Once a person's selfie is captured and transmitted, facial age estimation processing "takes on average less than one

[5] Federal Trade Commission, Letter Re: Imperium, LLC Proposed Verifiable Consent Method Application (FTC Matter No. P135419) (2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf.
[6] ESRB Group Application at 7.
[7] *Id.* at 13.

second" and returns a simple yes/no result on whether the individual in the image meets a designated age threshold."[8]

The relatively frictionless nature of the ESRB group proposal could be particularly helpful if the need to establish a parent-child relationship becomes more ubiquitous as a result of new laws. Moreover, the proposal has the advantage of being privacy-protective by "not requir[ing] registration or any documentary evidence of the[] identity" of the person providing consent and immediately deleting the facial image used for age estimation.[9] The flip-side, though, is that these characteristics may make it easier, and potentially more likely, for a non-parent who happens to be over 25 to consent for a child.

The question the FTC must confront is whether estimating age alone in such a frictionless manner provides sufficient reliability that the person is the child's parent. In addressing that question, the FTC should consider the proposed method's potential use by nefarious actors to circumvent the other, more stringent verifiable parental consent mechanisms. For instance, imagine a scenario where an adult is grooming a child and wants to enable the child to access pornography. If the proposed method is approved, the grooming adult could use their own face to provide consent for the child to access that material. Because of the lack of friction or any information gathering, the groomer may be more willing to undertake that process than if they had to provide a government ID or otherwise have their identity confirmed.

The same could be true in other scenarios. Imagine a child who wishes to play a video game or watch a streamer playing a video game with a higher age rating than their parents allow for, where the stream is behind an age check. An older member of the household such as a sibling or nanny who does not agree with the parental rule could use their facial image to provide access to the child.

[8] *Id*. at 4-5.

[9] *Id.* at 10. The most secure system would perform the analysis on the device itself, never storing or sending the facial image or face print anywhere, and would simply communicate an age range or a yes/no answer to the requester. As no user data would leave the user device, this would minimize data leakage risks. However, on-device computation might be infeasible due to processing power requirements or inequitable if it functions only on newer phones. In that case, a secure system would ensure that images or faceprints are properly encrypted and transmitted securely, and deleted from the company's servers once the analysis is completed. Given that this proposal is for the use of this type of technology rather than a specific system implementation, if the FTC approves this approach, it should make clear what security standards must be met for its use across all implementations.

It is of course possible for nefarious or otherwise unauthorized actors to take advantage of almost any parental consent mechanisms (such as a telephone call, video call, or a physical signed consent form). However, the Commission needs to consider whether the lack of friction in this method specifically makes the likelihood of that materially higher than prior approved methods, and, if so, how to balance that against greater privacy protection for the person providing consent and ease of use.[10]

II. The Commission should also address risks of disparate outcomes for particular demographic groups. *(Questions 3 and 4)*

As Appendix C of the Application indicates, there is a greater incidence of false negatives in facial age estimation for female users who have a darker skin tone, as well as a higher rate of false positives for male users with darker skin tones.[11] To be sure, the applicants note that particularly the latter difference is relatively small. If the Commission agrees that the differences shown are not sufficient to indicate bias, it should still provide guidance on when such differences would become material and indicate bias in other implementations of this methodology.

For methods that incorporate facial analysis, it is also critical to examine whether the system is as effective for transgender and nonbinary people and disabled people. Systems that are designed and developed using more homogenous sets of facial images are less likely to produce accurate estimations for transgender people who may be taking puberty blockers, or people whose gender expression does not otherwise conform with how gender is represented in training datasets.[12] In addition, the systems may yield inaccurate results for people with disabilities that affect their facial features or structure, or disabilities that make it difficult to maintain eye contact with a smartphone camera, hold the camera steady, or otherwise navigate its use to successfully capture an effective selfie.[13] These risks should be identified and mitigated in any verification method before implementation.

[10] The balance of interests is different in the case of age verification or assurance, where greater privacy for the person whose age is being checked has more unequivocal benefit. Thus, whatever the Commission decides here with respect to parental consent should not necessarily apply to age verification or assurance.
[11] ESRB Group Application, Appendix C.
[12] Morgan Klaus Schueurman, Jacob M. Paul, and Jed R. Brubaker, *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, 3 Proceedings of the ACM on Human-Computer Interaction, Art. 144 (2019), https://dl.acm.org/doi/pdf/10.1145/3359246.
[13] Anhong Guo, Ece Kamar, Jennifer Wortman Vaughn, Hanna Wallach, and Meredith Ringel Morris, *Toward Fairness in AI for People with Disabilities: A Research Roadmap* 2, ACM ASSETS Workshop on AI Fairness for People with Disabilities (2019), https://arxiv.org/pdf/1907.02227.pdf.

Conclusion

While CDT takes no position on this proposal, we urge the Commission in evaluating the proposal to consider the implications both for COPPA and in other contexts of determining that evidence that a person is old enough to be a child's parent is itself sufficient to reasonably establish that the person is actually the parent.