1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

August 21, 2023

Ms. April Tabor
Secretary
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex P)
Washington, D.C. 20580

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

On behalf of the Future of Privacy Forum (FPF), we are pleased to provide comment to the U.S. Federal Trade Commission regarding the use of "Privacy-Protective Facial Age Estimation" as a potential mechanism for verifiable parental consent under the Children's Online Privacy Protection Act (COPPA) Rule.[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.[2] In June, FPF published "The State of Play: Is Verifiable Parental Consent Fit for Purpose?," investigating the shortcomings and opportunities presented by the current framework for verifiable parental consent (VPC) under COPPA and encouraging ingenuity to address key challenges.[3] As federal lawmakers seek more comprehensive ways to update the 1998 law to match the 2023 online landscape, the approval of a new method for obtaining VPC has the potential to improve a process that is grappling with changing technologies, business practices, and individuals' expectations. This application for approval of a new method for obtaining VPC

[1] Entertainment Software Rating Board et. al., *Application for Approval of a Verifiable Parental Consent Method Pursuant to the Children's Online Privacy Protection Rule 16 C.F.R.§312.12(a),* Federal Trade Commission (June 2, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Application-for-a-new-VPC-method-ESRB-SuperAwesome-Yoti-06-02-2023.pdf.

[2] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board. The applicants in Project No. P235402 are FPF Advisory Board members and general support annual donors. FPF did not receive support for our work regarding our comments on this application from any donors.

[3] *The State of Play: Is Verifiable Parental Consent Fit for Purpose?*, Future of Privacy Forum (June 22, 2023), https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf.

presents the first opportunity since 2015 for the Federal Trade Commission (FTC) to review such an application.

It is critical to situate the proposed application for the use of age estimation technology to obtain VPC within the appropriate context. FPF's comments are limited to considering how this technology could improve the current VPC scheme; previous FPF analysis determined that "current methods of obtaining VPC may not achieve COPPA's goals in terms of efficacy and outcome [and] additional methods of obtaining VPC, particularly to allow more flexibility, should be explored."[4] The technology in this application estimates the ages of parents - not children - and serves as one part of COPPA's larger regulatory framework.

Many stakeholders are currently weighing the potential impacts of age assurance, estimation, verification, and related technologies in various contexts, including proposals that would encourage or mandate use of age assurance technologies for all users of child-directed, mixed-audience, or general audience onlines services. However, FPF's comments do not discuss the merits of using technology as a method of age estimation or verification for *all* users of a child-directed or mixed-audience service, which may place disproportionate privacy risks and burden on all users. Rather, we confine our analysis to the proposed context of this application - Project No. P235402 - which we understand to only refer to the limited use of verifying that a purported parent granting COPPA consent is, in fact, an adult .

With COPPA's VPC framework in mind, we observe:

1. The "Privacy-Protective Facial Age Estimation" technology may improve the existing landscape for verifiable parental consent, provided appropriate privacy safeguards are in place;
2. The "Privacy-Protective Facial Age Estimation" technology and associated risks are distinct from the biometric privacy risks associated with facial recognition technologies; and
3. If the FTC approves the application, the Commission's approval should require ongoing implementation of the privacy and fairness safeguards outlined in the application.

The "Privacy-Protective Facial Age Estimation" technology may improve the existing landscape for verifiable parental consent, provided appropriate privacy safeguards are in place

COPPA requires operators of child-directed services to choose a method or methods "reasonably designed in light of available technology" to ensure that the child's parent gives consent to data collection and use. The consent mechanisms listed in the COPPA rule and approved by the FTC are widely used by organizations because they provide certainty and mitigate legal and other

[4] *Id.*

risks. To varying degrees, these existing VPC options present points of friction for both parents and children. While these points of friction exist with the intent to keep children safe online, in practice they remain an imperfect solution to the challenge of facilitating developmentally-appropriate online experiences for children. Concerns range from accessibility - not all parents have equal or easy access to the tools required - to efficacy - the methods available do not always produce appropriate results and may lead to frustration or encouragement of children to access services meant for adults.[5]

The new application for "Privacy-Protective Facial Age Estimation" presents a solution that could build on the most recent addition to the approved VPC methods. In 2015, the Commission approved Face Match to Verified Photo Identification (FMVPI) technology, which involves verifying a photo ID submitted by a parent against a second photo submission using facial recognition technology. The Commission noted that this method "is more rigorous" than existing approved methods because "it involves the use of facial recognition technology to check that the individual to whom the identification was issued is the same individual who is interacting with the system at that moment."[6] Commenters noted that the FMVPI created potential privacy risks arising from the collection and use of unique biometric identifiers. Unlike FMVPI, the currently-proposed "Privacy-Protective Facial Age Estimation" method eliminates the need for the parent to submit government-issued identification, or any other type of identifying information. This raises fewer privacy concerns while retaining the technology's ability to make accurate inferences about an individual's age.

The application for "Privacy-Protective Facial Age Estimation" proposes analyzing the geometry of a user's face to estimate with a high level of certainty that the individual is an adult. This June, FPF released a new infographic where the efficacy of age estimation through "facial characterization" is among the methods of age assurance scrutinized.[7] FPF's findings indicate that facial characterization is best suited to place users in age bands, or signal that a user meets an age threshold, such as under 13 or 21+. This functionality aligns with the proposed application for use, so long as a buffer is maintained to address concerns caused by age estimation of individuals on the threshold, as the technology is less effective for discerning age in a narrow

---

[5] *Id.* Additional methods include: signing a physical consent form and sending it back via fax, mail, or electronic scan; using a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder; calling a toll-free number staffed by trained personnel; connecting to trained personnel via a video conference; providing a copy of a form of government-issued ID that the operator checks against a database, as long as that identification is deleted from internal records upon completion of the verification process; answering a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer; and verifying a picture of a driver's license or other photo ID submitted by the parent, and then compare that photo to a second photo submitted by the parent, using facial recognition technology.

[6] Donald S. Clark, *Jest8 Limited's (Trading As Riyo) Application for Approval of a Verifiable Parental Consent Method,* Federal Trade Commission (November 18, 2015), https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf.

[7] Bailey Sanchez and Jim Siegl, *Unpacking Age Assurance: Technologies and Tradeoffs,* Future of Privacy Forum (June 26, 2023), https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf.

range like 17 versus 18. The application addresses this by using age 25 as the threshold. It is also noteworthy that the image is deleted immediately after conducting the age estimation without any secondary uses. This is a privacy risk mitigation practice and thus a critical component of the applicant's proposal. As the applicants explain:

> *[The technology] does not require registration or any documentary evidence of [parent] identity. It does not retain any information about parents, including their images. The images are not stored, viewed by humans, shared, used for any other purpose, or sold. Privacy-Protective Facial Age Estimation simply estimates a parent's age and then deletes the image almost immediately. Furthermore…the images are not used to train the model further.*

There must be proper guardrails in place to ensure that any future companies using facial age estimation technology as a VPC method align their privacy practices with those outlined in the proposed application. There is precedent for this, as the FTC letter of approval of the FMVPI method notes that "in order to use this method, companies must follow the conditions set forth herein…approval of the proposed method is conditioned on adherence to these conditions."[8] Companies developing products to provide age estimation should ensure the technology is well-tested and maintain responsible operational controls.

The "Privacy-Protective Facial Age Estimation" technology proposed and associated risks are distinct from the biometric privacy risks associated with facial recognition technology

While the FTC weighs the risks associated with this technology against its benefits, it is crucial to distinguish between facial characterization and facial recognition technologies.[9] While facial recognition aims to identify or verify a specific individual by comparing their unique biometric features against a database of known identities, facial age estimation focuses on analyzing and categorizing visual attributes of an individual's face to predict age range based on insights from aggregated data. It does not uniquely identify an individual nor does it require the collection or storage of unique biometric identifiers.

Assuming all information provided in the application is accurate, the data collected by the facial age estimation technology is unlikely to be considered "biometric" under most data privacy laws, including the Commission's recent Policy Statement.[10] This is because the technology is not used to determine identities, face scans are not retained, and individuals do not provide any

[8] Donald S. Clark, *Jest8 Limited's (Trading As Riyo) Application for Approval of a Verifiable Parental Consent Method,* Federal Trade Commission (November 18, 2015), https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf.

[9] See, Brenda Leong, "Understanding Facial Detection, Characterization and Recognition Technologies," Future of Privacy Forum (Sept. 2018), https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf

[10] "Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act," Federal Trade Commission (May 18, 2023).

information that could connect the facial scans with individual's identities.[11] The Information Commissioner's Office (ICO) in the United Kingdom considered a similar proposal as a part of its Regulatory Sandbox and analyzed whether the proposed technology collected "Biometric Data" under Article 4 (14) of the General Data Protection Regulation (GDPR). The ICO determined:

> *Having considered how the age estimation tool works (as explained to us by Yoti) we have concluded that it can be distinguished from other facial recognition technology (FRT). It appears that Yoti is not using the tool for the purpose of uniquely identifying the individuals whose images are captured using the age estimation tool. Instead, it is being used to categorise them by age without uniquely identifying them*.[12]

Therefore, since facial age estimation technology does not collect "biometric information," risks associated with biometric facial recognition, such as identity theft and fraud, are typically absent. However, the technology is not completely without risk. In 2018, FPF developed a series of best practices outlining key principles for the responsible adoption of facial detection, characterization, and recognition technologies that were referenced in the application.[13] With facial characterization generally, FPF notes that there are risks with this nascent technology that should be considered, such as the possibility of discrimination, deepfakes, and consequences of inaccurate predictions.

The applicants took steps to mitigate these risks, including by "training data on a diverse set of ages and range of skin tones" and found that "[a]cross skin tones and gender, the [false positive rate] remains consistently well below 0.1%."[14] Applicants also require a "liveness test" to ensure the user is an actual person and not a static image in order to thwart attempts to spoof the

---

[11] See, Tatiana Rice, "When is a Biometric No Longer a Biometric," Future of Privacy Forum (May 2022) ("definitions in U.S. state biometric privacy laws and comprehensive data privacy laws largely limit the scope of "biometric information" or "biometric data" to data collected for purposes related to identification); Daichendt and Odell v. CVS Pharmacy, 22 CV 3318 (N.D. Ill. Dec. 2, 2022) (dismissing a case and finding that a facial characterization system did not collect "biometric identifiers" under the Illinois Biometric Information Privacy Act since the system did not determine identity, nor did the plaintiffs provide CVS "with any information, such as their names or physical or email addresses, that could connect the voluntary scans of face geometry with their identities").

[12] *Regulatory Sandbox Final Report: Yoti*, Information Commissioner's Office, (April 2022), https://ico.org.uk/media/for-organisations/documents/4020427/yoti-sandbox-exit_report_20220522.pdf.

[13] Brenda Leong, *Privacy Principles for Facial Recognition Technology in Commercial Applications,* Future of Privacy Forum (September 2018), https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf.

[14] Entertainment Software Rating Board et. al., *Application for Approval of a Verifiable Parental Consent Method Pursuant to the Children's Online Privacy Protection Rule 16 C.F.R.§312.12(a),* Federal Trade Commission (June 2, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Application-for-a-new-VPC-method-ESRB-SuperAwesome-Yoti-06-02-2023.pdf.

system. As previously mentioned, the applicants set an acceptance threshold of age 25 to minimize the risk of false positives.[15]

Our analysis of "Privacy-Protective Facial Age Estimation" technology is limited to this specific use case and to well-tested technology that works on diverse populations and includes appropriate privacy measures, such as ensuring the technology does not uniquely identify individuals and requiring the photo to be immediately deleted. With the appropriate safeguards in place, this technology has the potential to modernize a dated process and help to facilitate compliance with the existing VPC requirements under COPPA. If the FTC approves the application, we urge the Commission's approval to require ongoing implementation of the privacy and fairness safeguards outlined in the application.

Thank you for this opportunity to comment on the proposed application.

Sincerely,

Jamie Gorosh, Senior Counsel
Bailey Sanchez, Senior Counsel
Jim Siegl, Senior Technologist
Tatiana Rice, Senior Counsel

The Future of Privacy Forum
https://fpf.org/

[15] *Id.*