Entertainment Software Rating Board
420 Lexington Avenue
Suite 2240
New York, NY 101070

SuperAwesome Ltd.
111 Buckingham Palace Road
London SW1W 0SR
United Kingdom

Yoti Ltd.
6th Floor, 107 Leadenhall Street
London EC3A 4AF
United Kingdom

June 2, 2023

April J. Tabor
Secretary
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580

RE: 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)

Dear Secretary Tabor:

Pursuant to Section 312.12(a) of the Children's Online Privacy Protection ("COPPA") Rule (the "COPPA Rule" or "Rule"),[1] the Entertainment Software Rating Board ("ESRB"), a COPPA Safe Harbor program, Yoti Ltd. and Yoti (USA) Inc. ("Yoti"), and SuperAwesome Ltd. ("SuperAwesome") (collectively, the "Applicants" or "we") request that the Federal Trade Commission ("FTC" or "Commission") approve a new verifiable parental consent ("VPC") mechanism known as "Privacy-Protective Facial Age Estimation," which is not currently enumerated in the Rule.

Privacy-Protective Facial Age Estimation (also "Facial Age Estimation") uses proven facial age estimation technology to analyze the geometry of a parent's face to confirm that they are an adult.[2] It comports with the criteria set out in Section 312.5(b)(1) of the Rule for new VPC mechanisms, and also reflects advances in digital technologies available since the Commission

[1] Children's Online Privacy Protection Rule, 16 C.F.R. § 312, issued pursuant to the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506 (1998).

[2] The term "parent" includes a legal guardian, as defined in § 312.2 of the COPPA Rule.

last approved a VPC method in 2015. Privacy-Protective Facial Age Estimation provides an accurate, reliable, accessible, fast, simple and privacy-preserving mechanism for ensuring that the person providing consent is the child's parent. Indeed, as the Applicants' experience with this facial age estimation technology demonstrates, it can be implemented in a way that is consistent with COPPA's data minimization (§ 312.7), confidentiality, security, and integrity (§ 312.8), and retention and deletion (§ 312.10) provisions, as well as the Commission's concerns about potential bias and discrimination.

The Applicants bring together a breadth of experience in privacy matters and technical expertise to submit Privacy-Protective Facial Age Estimation as a VPC mechanism. The ESRB is the non-profit, self-regulatory body for the U.S. video game industry. Since 2001, ESRB's privacy compliance and certification program, ESRB Privacy Certified ("ESRB Privacy Certified") has been one of a small number of programs approved by the FTC as a Safe Harbor under the COPPA Rule.[3] Yoti is a digital identity company that offers identity verification, age assurance, reusable digital identity, and e-signature solutions around the world. SuperAwesome, acquired by Epic Games in September 2020, is one of the world's leading providers of "kidtech"—technology and services (such as its Kids Web Services ("KWS") platform), which facilitate developers' compliance with the parental consent requirement of privacy laws like COPPA and the European Union's General Data Protection Regulation ("EU GDPR" or "GDPR"). SuperAwesome is a member of ESRB Privacy Certified.

Summary

This application for a new VPC method provides a description of facial age estimation technology and details how this proposed method meets the requirements of the COPPA Rule. It includes evidence from Yoti's testing, SuperAwesome's experience with parental consent flows deployed outside the United States, and assessments from international regulators. It also includes a comparison of facial age estimation with other VPC methods previously approved and rejected by the Commission.

Our application is divided into two main sections:

I. A description of the facial age estimation technology pioneered by Yoti, its use in Applicants' proposed verifiable parental consent method, and a description of current implementations.

II. An analysis of how the Privacy-Protective Facial Age Estimation technology meets the requirements set forth in Section 312.5(b)(1) of the COPPA Rule and comports with the underlying purposes of COPPA; specifically, that the method:

   A. constitutes a new methodology not covered by those already enumerated in Section 312.5(b)(2) of the Rule;

[3] As an FTC-authorized COPPA Safe Harbor, the ESRB has the authority, under Section 312.5(b)(3) of the Rule, to "approve its member operators' use of a parental consent method . . . where the safe harbor program determines that such parental consent method meets the requirements of [Section 312.5(b)(1)]." Given the intense interest in child's privacy and the ongoing COPPA Rule review, rather than independently making such a determination, the ESRB joins in this application with SuperAwesome and Yoti, seeking Commission approval for a new VPC method.

B. is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent;

C. protects and promotes children's privacy, does not present any substantial risk to parents' privacy, and addresses issues of bias and discrimination as well as inclusion.

The application also contains the following appendices:

A. The Applicants and Disclosure of their Relationships

B. Example of Implementation of Facial Age Estimation for VPC

C. Evidence of Accuracy, Success Rate, Effectiveness, Fairness and External Validation of Yoti's Facial Age Estimation

D. The Benefits of Facial Age Estimation in Terms of Parent Access and Choice

I. THE PROPOSED VPC METHOD: PRIVACY-PROTECTIVE FACIAL AGE ESTIMATION TECHNOLOGY

A. How Facial Age Estimation Technology Works

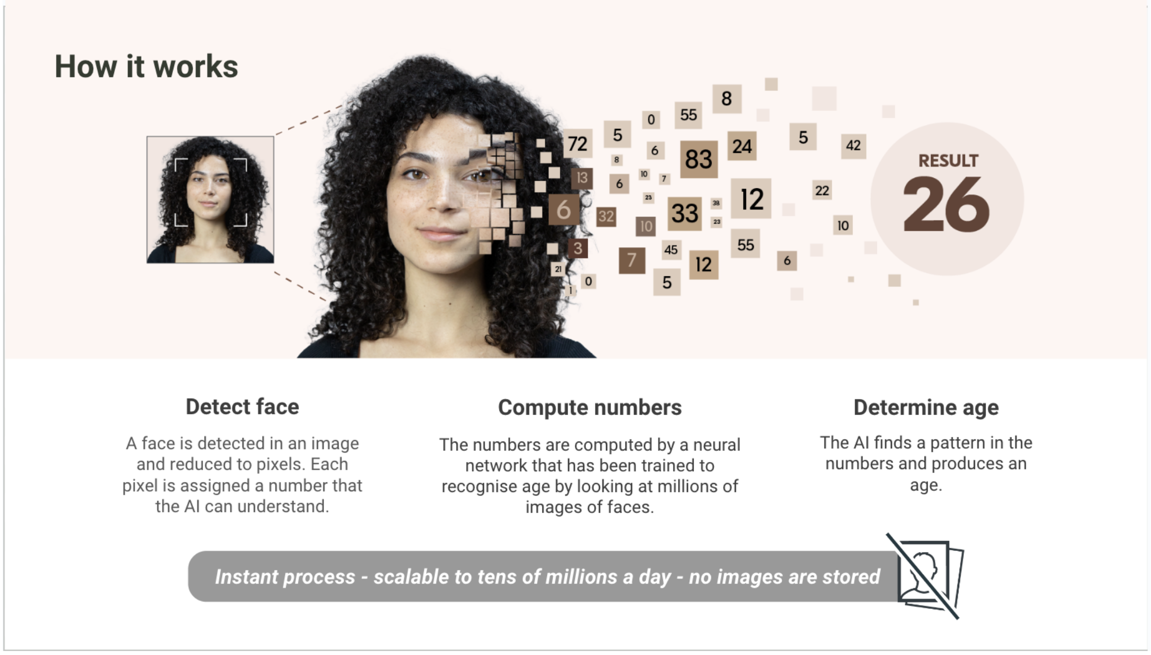
Facial age estimation uses computer vision and machine learning technology to estimate a person's age based on analysis of patterns in an image of their face. The system takes a facial image, converts it into numbers, and compares those numbers to patterns in its training dataset that are associated with known ages. By contrast, facial *recognition* technology, which seeks to identify a specific person based on a photo, looks for unique geometric measures of the face, such as the distance and relationship among facial features, and tries to match these to an existing unique set of measurements already recorded in a database along with unique identifying information.

In Yoti's case, the company trains its neural network model by feeding it millions of images of diverse human faces with their actual month and year of birth.[4] The system converts the pixels of these images into mathematical functions that represent patterns. Over time, the system has learned to correlate those patterns with the known age.

When performing a new age estimation, the system extracts the portions of the image containing a face, and only those portions of the image are analyzed for matching patterns. To match patterns, each node in Yoti's neural network performs a mathematical function on the pixel data and passes the result on to nodes in the next layer, until a number finally emerges on the other side. The only inputs are pixels of the face in the image, and the only outputs are numbers. Based on a review of the number patterns, the system creates an age estimation.

[4] Yoti collected its training data in accordance with the EU GDPR via the Yoti app. The Yoti app is a secure digital ID application that allows consumers to store their identification documents in one securely encrypted place, and to share that information (or share only the relevant attributes, such as age) with a business. The app has been downloaded 13 million times. For more information on how Yoti collects and handles model training data, *see* Yoti, *Facial Age Estimation: White Paper* at 27 (Mar. 2023) ("Data used to build the model ('training data')"), https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-March-2023.pdf ("Yoti White Paper").

The following diagram from the *Yoti White Paper* illustrates this process:[5]



Detect face

A face is detected in an image and reduced to pixels. Each pixel is assigned a number that the AI can understand.

Compute numbers

The numbers are computed by a neural network that has been trained to recognise age by looking at millions of images of faces.

Determine age

The AI finds a pattern in the numbers and produces an age.

Instant process - scalable to tens of millions a day - no images are stored

Although an individual's age may be considered an attribute of their identity, establishing the identity of an individual is not necessary to gain age assurance. Because the only data used to train the model are face images and the person's age in months and years, the model cannot work out anything other than the person's estimated age.

When using Privacy-Protective Facial Age Estimation, the user takes a photo of themselves (a selfie) assisted by an auto face capture module that guides the positioning of their face in frame. The system then checks whether there is a live human face in the frame and requires the image to be captured in the moment.[6] The upload of still images is not accepted, and photos that do not meet the required level of quality to create an age estimate are rejected. These factors minimize the risk of circumvention and of children taking images of unaware adults.[7]

The captured image is securely transmitted from the user's device to the Yoti backend server for age estimation processing using TLS 1.2 encryption.

[5] *Yoti White Paper*, *id*. at 20.

[6] This proprietary anti-spoofing technology has been tested and approved by the National Voluntary Laboratory Accreditation Program of the United States' National Institute of Standards and Technology (NIST). For more information, *see* National Voluntary Laboratory Accreditation Program (NVLAP), https://www.nist.gov/nvlap.

[7] For more information about how Yoti's anti-spoofing technology works, *see* Yoti, *Yoti MyFace Liveness: White Paper* (Mar. 2023), https://www.yoti.com/wp-content/uploads/Yoti-MyFace-Liveness-White-Paper-March-2023.pdf.

The processing takes on average less than one second. For the use case of parent verification, the operator receives only a yes/no result on whether the individual in the image meets a designated age threshold. If the image does not meet the age threshold, the individual may be permitted to restart the verification process (as configured by the operator). Images are immediately, permanently deleted, and not used by Yoti for training purposes.

B. Current Implementation of Privacy-Protective Facial Age Estimation for Legally Required Parental Consent Outside the US

Yoti and SuperAwesome have implemented the Privacy-Protective Facial Age Estimation method for legally required parental consent in territories outside the U.S. and have—since 2022—delivered more than 4.8 million age estimations using this method for this purpose.[8] The evidence from this international experience with Privacy-Protective Facial Age Estimation for parent verification supports approval as a VPC method:

- *Facial Age Estimation is accurate* – in the Applicants' implementation the facial age estimation system correctly estimates that someone is an adult 99.97% of the time.[9] *See* Appendix C, Accuracy.
- *Facial Age Estimation is effective* – on average 35% of users in the EU and U.K. who attempt to prove they are adults are rejected for being under the threshold age (they can choose another method if they disagree). *See* Appendix C, Effectiveness.
- *Facial Age Estimation is private* – it requires no collection of identity or payment card information, and no images are stored. *See* Section II.C, Parents' Privacy.
- *Facial Age Estimation is inclusive* – everyone has a face, but not everyone has a payment card, passport, driver's license or social security number (SSN). *See* Appendix D, Parent Access and Choice.
- *Facial Age Estimation is equally, or more, reliable than existing methods* – when combined with a liveness test, face scan is very difficult to spoof. *See* Appendix C, Success Rate.
- *Facial Age Estimation is preferred by users* – when given a choice of three methods, generally over 70% of users choose facial age estimation. *See* Appendix D, Parent Access and Choice.
- *Facial Age Estimation is easier to use* – 91%+ of users who start the face scan flow complete it, as compared to 65% for payment cards, or 66% for SSN. *See* Appendix C, Success Rate.

SuperAwesome's Kids Web Services ("KWS") currently deploys Facial Age Estimation in its parental consent tool as a verification method that developers can choose to make available to parents outside the U.S. alongside other methods, such as payment card or identity documents scan. Developers integrate KWS' parent verification (PV) module with their existing parental

[8] Analytics data from KWS and Yoti, since 2021, across multiple customer implementations worldwide. For more information about Kids Web Services, including examples of current live customer implementations, *see* https://dev.superawesome.com/.

[9] The proportion of those estimated to be over the configured threshold of 25 who are in fact adults (18 or older).

permissions flow, typically adding it at the end to verify that the person providing the permissions is an adult.

Examples of legally required parental consent flows powered by KWS, which use Facial Age Estimation, can be seen live in the account creation flows (outside the U.S.) of SuperAwesome KWS customers, including Epic Games.

For use as a COPPA VPC method, Privacy-Protective Facial Age Estimation can be deployed as follows:

1. Child visits an online service and is presented with a neutral age gate.
2. Operator collects a parent's email address from the child.
3. Operator sends direct notice to parent pursuant to Section 312.4(c) of the COPPA Rule.
4. Parent provides relevant permissions for the child.
5. Operator informs parent of the requirement to verify they're an adult; offers parent a choice of verification methods.
    a. Parent selects Privacy-Protective Facial Age Estimation.
    b. Parent is given notice of how facial age estimation works and provides consent for the collection of a face scan for the purpose of VPC.
    c. Parent provides consent to access the camera on their device.
    d. Parent presents face to the camera, the system performs a liveness test and takes a selfie.
    e. Age estimation takes place and collected image is deleted.
    f. System provides results of age estimation to operator, confirming whether the parent is over the configured age threshold.
6. If Facial Age Estimation concludes the person is not an adult, then one of the following will occur (depending on the operator's configuration):
    a. If the person is estimated as being 18-25, or there is some other uncertainty about whether the person is an adult, the person is returned to the beginning of step 5, where they can choose an alternative verification method that uses additional personal information, such as a payment card, driver's license or SSN.
    b. If the person is estimated as being under the age threshold, the operator will inform the person that VPC is denied and direct them to contact the operator's customer support if they disagree with the result or believe there was a technical error.

See *Appendix B* for mockups of the above VPC flow using Facial Age Estimation for parent verification. This flow is identical to current live implementations of KWS VPC in the U.S., up to the point of introducing Facial Age Estimation as an additional, optional verification method.[10]

[10] KWS' current VPC flow as implemented in the U.S., which uses payment card and SSN as verification methods, has been certified as COPPA-compliant by two FTC-authorized Safe Harbor Programs: (i) co-applicant ESRB Privacy Certified and (ii) Kidsafe.

II. THE PROPOSED FACIAL AGE ESTIMATION TECHNOLOGY METHOD MEETS THE CRITERIA OF THE COPPA RULE AND ADDRESSES OTHER PRIVACY CONCERNS

Applicants' proposed method meets the criteria set out in Section 312.5(b)(1) of the COPPA Rule for approval of a new VPC method. First, the proposed method is distinct from existing methods set out in the COPPA Rule, including the two methods last approved by the Commission. Second, it is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. In addition, the method promotes children's privacy, does not present any substantial risk to parents' privacy, and addresses issues of potential bias and discrimination as well as inclusion.

A. The Proposed Method is Distinct From Existing Methods Set Out in the COPPA Rule.

The Privacy-Protective Facial Age Estimation proposed by Applicants is unique, and distinct from the other methods set out in the COPPA Rule. To date, the Commission has not approved a VPC method that involves facial analysis without requiring additional personal information.[11]

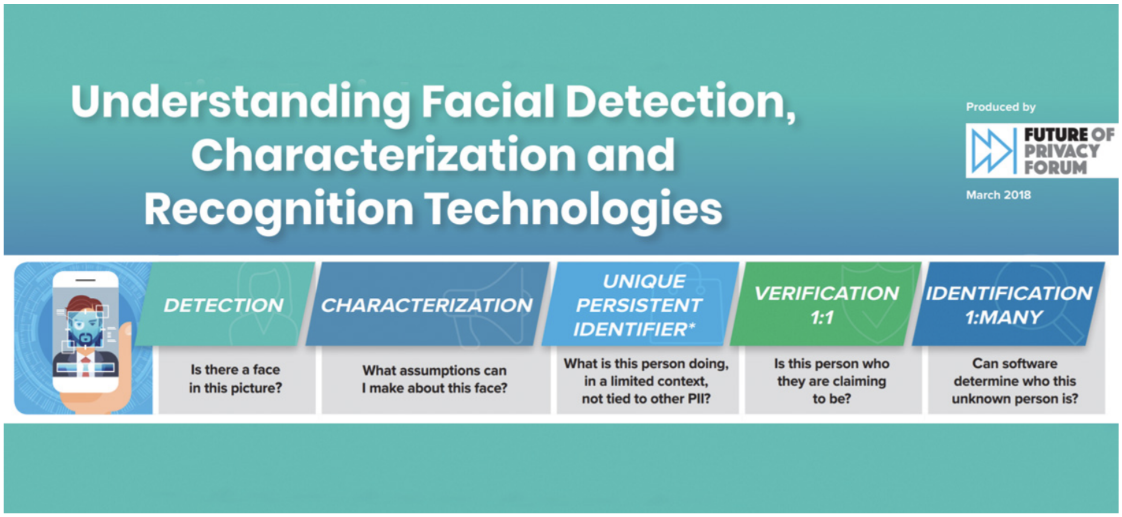
The only method that is arguably similar is the "Face Match to Verified Photo Identification" (FMVPI) method that the Commission approved in 2015. FMVPI is a two-step facial recognition process that compares a photo in a parent's government-issued ID (for example, a driver's license or passport) with an image of the parent taken with the parent's device. Although both the Facial Age Estimation and the FMVPI method use some form of facial analysis technology, the similarity ends there.

FMVPI is an image-matching method, not a facial age estimation method. FMVPI requires the parent to submit personal information and a photo to perform the one-to-one match, whereas Facial Age Estimation preserves privacy by not requiring the parent to produce additional identity documentation or information. Facial Age Estimation 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.

In its infographic on *Understanding Facial Detection, Characterization and Recognition Technologies*, the Future of Privacy Forum (FPF) graphically showed the critical distinction – in terms of privacy-preservation – between various uses of facial analysis technologies:[12]

[11] Co-applicant ESRB Privacy Certified, in its 2019 comment in the COPPA Rule Review, recommended that the FTC modernize VPC mechanisms by allowing the incorporation of fingerprint and facial recognition, especially because those features are often on a parent's mobile device. ESRB, *Comment Letter on COPPA Rule Review* (Dec. 10, 2019), https://www.regulations.gov/comment/FTC-2019-0054-116012.

[12] Brenda Leong, *FPF Releases Understanding Facial Detection, Characterization, and Recognition Technologies and Privacy Principles for Facial Recognition Technology in Commercial Applications*, Future of Privacy Forum (Sept. 20, 2018), https://fpf.org/blog/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/.



Understanding Facial Detection, Characterization and Recognition Technologies

Produced by FUTURE OF PRIVACY FORUM

March 2018

DETECTION — Is there a face in this picture?

CHARACTERIZATION — What assumptions can I make about this face?

UNIQUE PERSISTENT IDENTIFIER* — What is this person doing, in a limited context, not tied to other PII?

VERIFICATION 1:1 — Is this person who they are claiming to be?

IDENTIFICATION 1:MANY — Can software determine who this unknown person is?

The Privacy-Protective Facial Age Estimation method as proposed uses only the first two factors (detection and characterization) in which no personal information is retained. This differs from other uses of facial analysis, including the FMVPI method, which applies 1:1 recognition to confirm a match between the live and documented identities of a person. As the Commission itself acknowledged in approving the FMVPI method, the FMVPI method was “very similar” to the government documentation method already included in the Rule.[13]

Nonetheless, the Commission recognized that the FMVPI method, which incorporated new technology into the process of verifying an identity document (as previously permitted) was distinct enough to meet the requirements of the COPPA Rule.[14] Likewise, Facial Age Estimation is distinct from the other methods set out in the Rule.

B. The Proposed Method is Reasonably Calculated, in Light of Available Technology, to Ensure that the Person Providing Consent is the Child’s Parent.

Privacy-Protective Facial Age Estimation provides a very high level of assurance that the person providing the consent is old enough to be a parent. It uses available technology to achieve the balance of making it easy for the parent to provide consent, while making it difficult for the child (or even an older sibling) to pose as the parent. It therefore meets the Rule’s requirement that “Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.”[15]

[13] Letter from Donald S. Clark, Secretary, F.T.C., to Allison Fitzpatrick, Jest8 Limited (trading As Riyo) (Nov. 18, 2015), https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf (“FMVPI Letter”).

[14] *Id.*

[15] COPPA Rule, § 312.5(b)(1).

All the currently approved VPC methods establish that the person is an adult; none of them definitively authenticates the parent-child relationship.[16] The COPPA Rule, nonetheless, permits these methods in line with the Rule's qualification that new VPC methods be held to the standard of "reasonably available technology," not a requirement of perfect, still-to-be developed, solutions.

Indeed, in approving the application for the FMVPI method, the Commission explicitly rejected one commenter's assertion that "children can easily circumvent the system because the . . . system <u>authenticates the identity of the holder, not the parent-child relationship</u>."[17] The Commission explained its reasoning by pointing to its previous decision to allow government-issued ID as an enumerated VPC method. There, the Commission explained that the approved method "reasonably ensures that the person providing consent is the parent."[18]

Moreover, children cannot easily circumvent Facial Age Estimation, which requires the live participation of an adult who is old enough to be the child's parent to submit to the process. A child's 14-year-old sibling or 18-year-old babysitter, for example, would not be able to pass the Facial Age Estimation process. This makes it more likely that the person going through the age estimation flow is the child's parent.

The Privacy-Protective Facial Age Estimation method therefore differs significantly from proposed methods disallowed by the FTC, such as digital signature, because they would be easy for a child to circumvent. In rejecting AgeCheq's proposed VPC method, which involved the collection of the parent's personal information followed by a process for a digital signature using a validation code, the Commission explained:

> AgeCheq's proposed . . . method does not add further indicia of reliability because it does not verify the identity of the parent – it authenticates the device rather than the user. A significant number of children under 13 have their own smartphones. Moreover, a child could at any given time be using the parent's device and interacting with a particular app. Given such access, a child could easily obtain a validation code from AgeCheq (or another intermediary or operator who uses the proposed method) by inputting a name, address, and (made up) birth year into the very device that the child is using to download the app.[19]

The Facial Age Estimation proposed here, by contrast, is not easy for a child to manipulate. The configuration of a high threshold age of 25 and built-in requirement of liveness provide

[16] *See* Yoti Response to the Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule (Responses to Q.1a and Q.7) (Mar. 22, 2020), https://www.regulations.gov/comment/FTC-2019-0054-113202.

[17] FMVPI Letter, supra n. 24 (emphasis added). The Commission also rejected the argument the FMVPI method did not "verify that the parent has actually seen and consented to their child's data being collected and shared, and that an opt-out of data collection should be in place," explaining that "[t]his is true of other VPC methods already approved under the Rule." *Id*.

[18] 78 Fed. Reg. 3972 (Jan. 17, 2013), https://www.ftc.gov/policy/federal-register-notices/childrens-online-privacy-protection-rule-final-rule-amendments ("2013 SBP").

[19] Letter from Donald S. Clark, Secretary, F.T.C. to Roy R. Smith, II, CEO, AgeCheq Inc. (Jan. 27, 2017), https://www.ftc.gov/system/files/documents/public_statements/621461/150129agecheqltr.pdf.

important safeguards.[20] It is analogous, in that respect, to the FMVPI method (discussed above) and the government documentation method previously approved by the Commission.[21]

As the decade since the Rule was last amended has demonstrated, it is very difficult to implement a way of verifying parental identity that is failsafe, privacy-protective, and cost-effective. The Facial Age Estimation proposed here more than meets the standards that the Commission has previously used to approve new VPC methods in line with the COPPA Rule.

C. The Proposed New VPC Method Protects and Promotes Children's Privacy, Does Not Present Any Substantial Risk to Parents' Privacy, and Addresses Issues of Bias and Inclusion.

Facial Age Estimation is designed with privacy and data minimization in mind for both children and parents. It protects and promotes children's privacy by providing a reliable, accessible and simple method for operators to obtain VPC, so they can deliver appropriate experiences to users under the age of 13. It does not involve any collection of information from the child apart from the parent's email, which the COPPA Rule recognizes may be necessary to obtain VPC.[22]

The Facial Age Estimation method also protects parents' privacy. It does not require registration or any documentary evidence of their 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, in Yoti's deployment of Facial Age Estimation for VPC, the images are not used to train the model further. To Applicants' knowledge, there is no reason that other companies developing similar facial estimation methods could not adopt the same protocol. Indeed, the Commission has previously made clear that companies seeking to use a Commission-approved VPC method must incorporate the same privacy-protective standards as the originally approved method.[23]

[20] In the Applicants' current (and proposed) implementation, the pass/fail threshold for establishing adulthood is set at 25 in order to minimize the likelihood of a minor passing off as an adult. This probability, known as the False Positive Rate (FPR), is 0.03% when the threshold is set at 25; it is 0.4% when it is set at 21. The risk of false rejections of parents as a result of this higher threshold is extremely low, as 98.2% of mothers of 6+ year olds are over 25, based on CDC data. *See Appendix C, Accuracy* for more detail on these calculations.

[21] FMVPI Letter and 2013 SBP.

[22] Section 312.5(c)(1) permits online businesses to collect the name or online contact information of the parent or child when the sole purpose of such collection is to provide notice and obtain parental consent. The Rule further states that "[i]f the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records."

[23] In granting the application for the FMVPI method, the Commission dismissed an objection that the method might be implemented in a way that did not meet privacy standards. It explained:

> In order to use this method, companies must follow the conditions set forth herein. [The] application makes clear that information collected will be promptly destroyed and that the information will not be used for any other purpose. Approval of the proposed method is conditioned on adherence to these conditions.

See FMVPI Letter at 4.

Moreover, Yoti's Facial Age Estimation does not involve the processing of sensitive personal data such as health, or religious information, or information about children.[24] Again, this important privacy-protecting protocol could be adopted by other companies developing facial age estimation techniques for verifiable parental consent under COPPA.

Facial Age Estimation also addresses privacy-related issues such as inclusion as well as bias and discrimination.[25] Parents who do not have a social security number or a payment card can use the facial age estimation process. (For a more detailed analysis, see *Appendix D, Parent Access and Choice*.)

Additionally, Privacy-Protective Facial Age Estimation can be developed in a way that mitigates the potential for bias and discrimination based on gender or race. Yoti uses millions of faces to train its algorithm (collecting face image, month and year of birth only), regularly assessing the results of its age estimation mechanism by gender and skin tone. It seeks out specific, GDPR-compliant training data sets to fill any gaps in its coverage and to ensure that it includes a wide range of individuals. Yoti publishes its testing results.[26] The data suggests that

[24] In Europe, this data is referred to as "special category data." In October 2021, the U.K.'s ICO stated that age estimation "may" involve the processing of biometric data (at para 2.3.2); however, later in the report, it clarified (at para 4.2.1) that facial age estimation data is only biometric data when it is used to identify a unique individual. ICO, *Age Assurance for the Children's Code* (Oct. 2021), https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf.

In a subsequent report the ICO confirmed its view on the distinction between using biometric data for age estimation rather than identification: "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." [3.11] "We have concluded that Yoti's age estimation tool will not result in the processing of special category data." [4.2], ICO, *Regulatory Sandbox Final Report: Yoti* (Apr. 2022), https://ico.org.uk/media/for-organisations/documents/4020427/yoti-sandbox-exit_report_20220522.pdf.

[25] The FTC recently set out various concerns that biometric information technologies, such as those that process facial images, "can lead or contribute to harmful or unlawful discrimination." FTC, *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act* [hereinafter, *Biometric Information Policy Statement*] 4-5 (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf. The FTC has long stressed the importance of addressing unlawful bias and discrimination as well as other harms arising from data-intensive technologies. *See e.g.*, FTC, *Combatting Online Harms Through Innovation: A Report to Congress* (June 16, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf;
FTC, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. Just last month, the agency, along with officials from the Department of Justice (DOJ), the Consumer Financial Protection Bureau (CFPB), and the Equal Employment Opportunity Commission (EEOC) released a joint statement announcing the agencies' resolve to monitor automated systems for bias and discrimination and "vigorously use our collective authorities to protect individuals' rights regardless of whether legal violations occur through traditional means or advanced technologies." *See Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems* 3 (Apr. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

[26] Masha Borak, *Yoti improves accuracy and skin tone balance for age estimation: Approaches 600M age checks,* Biometric Update (Apr. 3, 2023), https://www.biometricupdate.com/202304/yoti-improves-accuracy-and-skin-tone-balance-for-age-estimation

Privacy-Protective Facial Age Estimation as implemented for parent verification is not materially impacted by variations in the accuracy of its estimations based on age, gender or skin tone. To be more specific, any variations in accuracy resulting from algorithmic bias are unlikely to impact the yes/no result of whether a user meets the age threshold set for parental verification. For more analysis on bias, see *Appendix C, Fairness*.

Further, Privacy-Protective Facial Age Estimation's use of facial scanning techniques does not pose a substantial risk to parents' privacy even when analyzed under laws and policies relating to "biometric information." In its recently announced *Biometric Information Policy Statement*, the Commission defined biometric information as follows:

> Biometric information includes, but is not limited to, depictions, images, descriptions, or recordings of an individual's facial features, iris or retina,finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern). Biometric information also includes data derived from such depictions, images, descriptions, or recordings, **to the extent that it would be reasonably possible to identify the person from whose information the data had been derived.** By way of example, both a photograph of a person's face and a facial recognition template, embedding, faceprint, or other data that encode measurements or characteristics of the face depicted in the photograph constitute biometric information.[27]

This broad definition encompasses many types of data but ultimately turns on whether the information – or data derived from it – could be used to identify an individual. Here, even though the Privacy-Protective Facial Age Estimation method works by processing a photograph of a face, the only output is a non-identifying age estimation. It is not therefore "reasonably possible" to identify the person from whose information the data had been derived."

Applicants recognize, however, that facial estimation scans can raise privacy concerns. These concerns can be addressed through the specific criteria included in the method the Commission approves, which can incorporate the practices set out in the *Biometric Information Policy Statement*. These include requiring providers to:

- Conduct a comprehensive evaluation of potential risks posed by collecting biometric data before doing so;
- Address known or foreseeable privacy risks, including risks of bias, error, or discrimination that could cause potential consumer injury;

[27] *Biometric Information Policy Statement*, supra n. 36 at 1 (emphasis added). Most state biometric laws similarly require that any information captured from a biometric "identifier" such as a facial scan be used to identify an individual in order to fall within the scope of statute. *Compare* California Consumer Privacy Rights Act, Cal. Civ. Code § 1798.100 *et seq*., as amended ("'Biometric information' means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, *to establish individual identity*" (emphasis added)), *with* Illinois Biometric Information Privacy Act, 740 ILCS § 14/10 ("'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual").

- Employ technical safeguards, such as timely updates on systems that capture, process, or store biometric information to ensure safe operation of these systems; and
- Clearly and conspicuously disclose the collection and use of biometric information and obtain legal consent when necessary.[28]

Moreover, the Privacy-Protective Facial Age Estimation flow can be customized by developers to include consent mechanisms that may be required in the relevant jurisdictions. The example implementation of Privacy-Protective Facial Age Estimation in *Appendix B* provides parents with the ability to review the method and opt-in to having their photo taken for this purpose, or to choose another method.[29] The Privacy-Protective Facial Age Estimation method, therefore, does not pose a substantial risk to parents' privacy because parents remain in control of what information they choose to share.

To the extent that there is any risk, it is easily outweighed by the benefits to consumers and businesses of using this method. Privacy-Protective Facial Age Estimation offers parents an easy way to provide VPC through a quick process, without needing to provide extensive personal information, in line with data minimization principles. It is efficient and cost-effective for businesses, and can be deployed widely. Finally, it can be used by parents who do not have government identification or do not own a payment card, thereby promoting access to COPPA's protections for some of the most vulnerable consumers.

[28] *See* supra n. 38 at 7. The *Biometric Information Policy Statement* also sets out other practices that companies should follow when handling data that falls within the FTC's definition of biometric information.

[29] This opt-in consent would meet the standard set by the Commission in the *Everalbum* matter, which settled the FTC's charges that Everalbum deceived its users about its use of facial recognition and improperly retained photos and videos from users who had deactivated their accounts. *See Everalbum, Inc.*, FTC Matter No. 192 3972 (last updated May 5, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3172-everalbum-inc-matter. In the final Decision and Order (FTC Docket No. C-4743 (May 6, 2021), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf, the FTC required the company, in the future, to obtain express affirmative consent for the use of biometric information, using a clear and conspicuous disclosure that, "separate and apart from any 'privacy policy,' 'terms of use' page, or other similar document, [explained] all purposes for which [Everalbum] will use, and to the extent applicable, share, the Biometric Information."

CONCLUSION

For the reasons stated herein, Applicants ESRB, SuperAwesome, and Yoti request that the Commission grant the application for a new verifiable parental consent method under Section 312.5(b) of the COPPA Rule.

Sincerely,

DocuSigned by:
Stacy Feuer
AE4BA658C250423... 02-Jun-23

Stacy Feuer
Senior Vice President
Entertainment Software Rating Board, Privacy Certified

DocuSigned by:
58553CB481094EB... 02-Jun-23

Max Bleyleben
Managing Director
SuperAwesome Ltd.

DocuSigned by:
Julie Dawson
9FA017433F6F44A... 02-Jun-23

Julie Dawson
Chief Policy & Regulatory Officer
Yoti Ltd.

APPENDICES

APPENDIX A: The Applicants and Disclosure of their Relationships

Yoti

Yoti was founded in 2014 with a mission to become the world's most trusted identity platform – enabling people to prove who they are and how old they are. Yoti's solutions span identity verification, age assurance, digital identity and e-signature solutions. One of Yoti's core innovations is the use of facial analysis for age estimation. Its Facial Age Estimation solution is used by regulated industries as well as gaming, retail, toy brands and public offices, to estimate the age of their visitors in order to tailor the user experience or to help organizations comply with the law.

Yoti Facial Age Estimation has proven particularly effective in establishing that an individual is an adult, not only enabling digital services to provide age-appropriate access to adult content or services, but also physical outlets to automate age checks in conjunction with restricted products. For example, supermarket checkout,[30] gaming machine outlets[31] and lottery terminals[32] find utility in using Yoti's terminal-based solution to enable age verification at the point of sale.

Yoti maintains contact with regulators and child protection bodies in countries developing legislation in this area, and was the first organization certified to the British Board of Film Classification's Age Verification Certificate scheme under the U.K.'s Digital Economy Act of 2017. This required Yoti's age verification services to adhere to very high standards for privacy and data security. Yoti Facial Age Estimation has been approved by the German Association for Voluntary Self-Regulation of Digital Media Service Providers (FSM Seal of Approval)[33] and by the Commission for the Protection of Minors in the Media (KJM)[34] to provide age verification services in Germany. Yoti Facial Age Estimation has been independently tested and certified by the U.K.'s Age Check Certification Scheme.[35]

[30] *See* The Kiosk Industry Group, *Age Verify via Facial Analysis - Aldi, NHS, NCR and Yoti* (Feb. 3, 2022), https://kioskindustry.org/age-verify-via-facial-analysis-aldi-nhs-ncr-and-yoti/.

[31] *See* Eve Kim Sing, *Regal Gaming Technologies and Yoti take new steps to protect young people: introducting digital age verification across UK bars, pubs and services stations*, Identity Week (Oct. 31, 2022), https://identityweek.net/regal-gaming-technologies-and-yoti-take-new-steps-to-protect-young-people-introducing-digital-age-verification-across-uk-bars-pubs-and-service-stations/.

[32] *See* Kesso Diallo, *La Française des jeux tests an AI to verify the age of players at tobacconists*, L'Éclaireur FNAC (Apr. 11, 2023), https://leclaireur-fnac-com.translate.goog/article/274244-la-francaise-des-jeux-teste-une-ia-pour-verifier-lage-des-joueurs-chez-les-buralistes/.

[33] *See* Yoti Press Release, *Yoti erhält Prüfsiegel der FSM für Technologien 'Age Scan' und 'Age Verification,'* (May 26, 2020), https://www.fsm.de/mitteilung/yoti-erhaelt-pruefsiegel-der-fsm-fuer-technologien-age-scan-und-age-verification/.

[34] *See* Yoti Press Release, *KJM bewertet sieben weitere Altersverifikationssysteme positiv* (Dec. 21, 2020), https://www.kjm-online.de/service/pressemitteilungen/meldung?tx_news_pi1%5Bnews%5D=4890&cHash=e45ae6dfeee26fcd23d10c6994b7a9ef.

[35] *Operational Acceptance Test (OAT): ACCS 0:2020 Technical Requirements for Age Estimation Technologies: Yoti AI Services Age API 1.1.1* (Nov. 20, 2020), https://www.accscheme.com/media/2ntishhf/age-estimation-results-executive-summary.pdf.

In the U.K., Yoti was selected to actively work with the Information Commissioner's Office, in the ICO Sandbox.[36] The partnership built customizable solutions to help other platforms and content communities meet regulatory requirements to protect children.

SuperAwesome

SuperAwesome is the leading provider of kidtech – technology and services used by companies worldwide to enable safe, privacy-compliant digital engagement with children. Founded in 2013, SuperAwesome has over 500 customers who use its technology across industries – including toy, film, consumer goods, entertainment and video games. Every month, SuperAwesome's platform enables billions of kid-safe transactions across video, advertising, community and parental consent. In September 2020, SuperAwesome joined the Epic Games group of companies.

Since 2015, SuperAwesome has operated a training and education program, Kidaware, designed to teach developers, publishers, brands and advertising agencies how to engage with children online in a privacy-compliant manner. The company also engages regularly with regulators in the U.K., Ireland, the U.S. and other countries on topics relating to children's privacy and technology solutions for age assurance and parental consent. In 2019, SuperAwesome submitted extensive comments to the FTC's regulatory review of the COPPA Rule, including a number of specific recommendations for improving the VPC requirement.[37]

Kids Web Services (KWS) is a platform provided by SuperAwesome to developers to facilitate their compliance with the parental consent requirement of privacy laws like COPPA and GDPR. Specifically, the Parent Verification module of KWS enables developers to verify that a parent is an adult in accordance with legally required parental consent, as applicable in various jurisdictions around the world. It does this by aggregating the most effective and appropriate verification methods available and enabling developers to present these methods to parents in a flow that is integrated into their service. Since 2021, KWS Parent Verification is provided completely free of charge to developers and publishers of all sizes.

KWS is certified under the COPPA Safe Harbor program by Entertainment Software Rating Board Privacy Certified and Kidsafe Seal.

The aim of KWS is to make it easier for developers to implement VPC, to improve the experience for parents going through VPC in order to increase parental engagement in their children's digital activities, and to reduce the incentive children have to circumvent age gates. Since 2015, KWS has powered 16m parent verifications using a range of parental consent methods, including those enumerated by the FTC under COPPA.

[36] *See* ICO, *ICO supports projects to strengthen children's privacy rights* (Jan. 15,2021), https://ico-newsroom.prgloo.com/news/ico-supports-projects-to-strengthen-childrens-privacy-rights.

[37] Letter from Max Bleyleben, Managing Director and CPO, SuperAwesome, to the FTC, (Dec. 9, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25091.

Entertainment Software Rating Board

Established in 1994 by the Entertainment Software Association, the ESRB is a non-profit, self-regulatory body that independently assigns age ratings for video games and mobile apps; educates parents about age ratings, parental controls, and related topics; enforces industry-adopted advertising guidelines; and works with major retailers to help ensure children are not sold video games rated for an older audience without a parent or guardian present.

In 1999, the ESRB saw an opportunity to further its self-regulatory mission by establishing an online privacy certification program to help companies in the video game industry adopt lawful, transparent, and responsible online privacy practices.[38] In April 2001, the Commission approved the ESRB's online privacy program as a Safe Harbor under COPPA.[39] Since then, the ESRB has continued to develop its Privacy Certified program, which now serves nearly 40 companies, including co-applicant SuperAwesome, in the United States and around the world, mainly in the video game and toy industries. They include multinational corporations, startups and non-profit organizations.

ESRB Privacy Certified members operate online services intended for a range of audiences, including some that are for users of all ages, some that are intended for parents or adults only, and some that are created specifically for children under the age of 13. The ESRB has two separate sets of program requirements: (1) the ESRB Privacy Certified Seal Requirements, which apply to all online services (i.e., websites, mobile apps, PC games, and internet-connected products) submitted to the program for certification that are not primarily directed to and do not target children, and (2) the ESRB Privacy Certified Kids Seal Requirements (the "Kids Seal Requirements"), which apply to online services directed or targeted to children. The Kids Seal Requirements, which are rooted in COPPA, are at the core of the ESRB Safe Harbor program.

Over the years, the ESRB has made changes to the COPPA Safe Harbor component of the Privacy Certified program to reflect changes in technology, law, and best practices for protecting children's privacy online. The Commission approved modifications to the ESRB's original COPPA Safe Harbor program in 2005, and again in 2013, in conformity with the FTC's amendments to the COPPA Rule.[40] In 2018, the ESRB submitted revised program requirements to the FTC to better align the program with the Commission's COPPA-related regulations and

[38] FTC, *Self-Regulation and Privacy Online: A Report to Congress* (July 1999), https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf.

[39] FTC Press Release, *Entertainment Software Rating Board Awarded "Safe Harbor" Status: Program Will Promote Compliance with Children's Online Privacy Protection Act* (Apr. 19, 2021), https://www.ftc.gov/news-events/news/press-releases/2001/04/entertainment-software-rating-board-awarded-safe-harbor-status.

[40] The Commission approved changes to the COPPA Rule in December 2012, which went into effect in July 2013. The Commission then approved the ESRB's revised COPPA Safe Harbor program when the revised COPPA Rule went into effect. *See* FTC Press Release, *Revised Children's Online Privacy Protection Rule Goes into Effect Today: FTC Continues Safe Harbor Programs, Expands Business and Parental Education Efforts* (July 1, 2013), https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect.

guidance. The FTC approved the revised program requirements, with modifications suggested by several privacy advocacy organizations, on August 13, 2018.[41]

The ESRB has continued to participate in discussions about strengthening children's online privacy and updating COPPA and the COPPA Rule. In 2019, the ESRB submitted extensive comments to the FTC's regulatory review of the COPPA Rule.[42] More recently, in November 2022, the ESRB filed a comment in response to the Commission's "Advanced Notice of Proposed Rulemaking on 'Commercial Surveillance and Lax Data Security Practices.'"[43] The ESRB drew on its experience as a COPPA Safe Harbor to suggest a multilayered, inclusive, and nuanced model for children and teen privacy.

Relationships among the co-applicants

SuperAwesome is a member of the ESRB's Privacy Certified program[44]. It has been engaged with the program since 2016, when it first submitted its Kids Web Services platform for review and certification under the FTC-authorized COPPA Safe Harbor. Since then, the ESRB has conducted biannual reviews of SuperAwesome's websites and other products. In addition, SuperAwesome consults with the ESRB on new features to ensure they are COPPA-compliant. Both organizations participate in joint working groups to consider innovations in age assurance, verifiable parental consent, and children's privacy.

Yoti and SuperAwesome have been working together since 2019 to explore the viability of Facial Age Estimation for verifiable parental consent. In 2021, one of SuperAwesome's largest clients, a market-leading toy company, began to use Yoti's Facial Age Estimation tool for legally required parental consent in Europe. When the company subsequently shifted all the parent verification for its global legally required parental consent flows onto the KWS platform in 2022, Yoti's Facial Age Estimation technology was integrated into KWS and made available as an option for all SuperAwesome clients.

In the course of 2022, other developers using KWS switched on Facial Age Estimation, including Epic Games. This led to more than 4.8m facial age estimations being conducted for legally required parental consent by SuperAwesome and Yoti since 2022. In early 2023, Yoti, SuperAwesome and ESRB Privacy Certified agreed to collaborate on this joint application to the FTC.

[41] Letter from Donald S. Clark, Secretary, FTC, to John M. Falzone, Vice President, ESRB (Aug. 13, 2018), https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-modifications-video-game-industry-self-regulatory-coppa-safe-harbor-program/p024526_commission_letter_approving_modified_esrb_program_and_exhibit_a.pdf.

[42] ESRB, *Comment Submitted by the Entertainment Software Rating Board to the COPPA Rule Review, 16 CFR Part 312, Project No. P195404* (Dec. 10, 2019), https://www.regulations.gov/comment/FTC-2019-0054-116012.

[43] ESRB, *Comment Submitted by the Entertainment Software Rating Board to the FTC's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Lax Data Security Practices, ANPR, R111004* (Nov. 21, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1117.

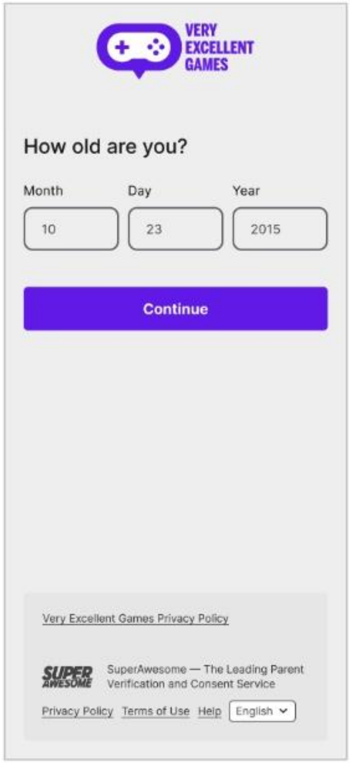
[44] *See* ESRB Privacy Certified Seal: Kids Web Services, https://www.esrb.org/EPCConfirm/887/.

APPENDIX B: Example of Implementation of Facial Age Estimation for VPC

Laid out below is a mockup of a VPC flow using Facial Age Estimation as an optional verification method. This flow is identical to the current live customer implementations of KWS in the U.S. up to the point where Facial Age Estimation is selected by the parent.

VPC Flow including Facial Age Estimation as PV method

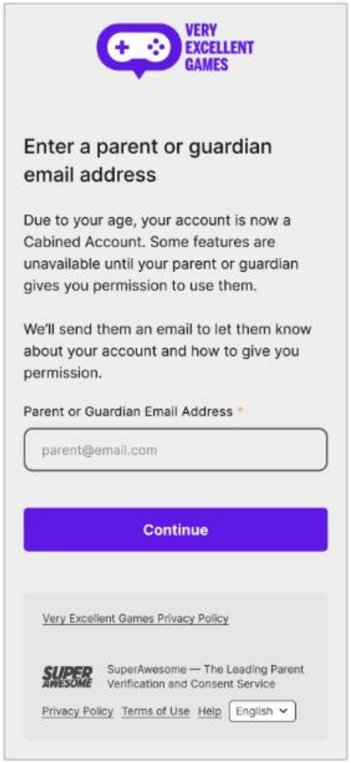
- Age gate
- Parent email collection
- Direct notice



How old are you?

Month: 10
Day: 23
Year: 2015

Continue
Very Excellent Games Privacy Policy
SUPER AWESOME
SuperAwesome — The Leading Parent Verification and Consent Service
Privacy Policy
Terms of Use
Help
English



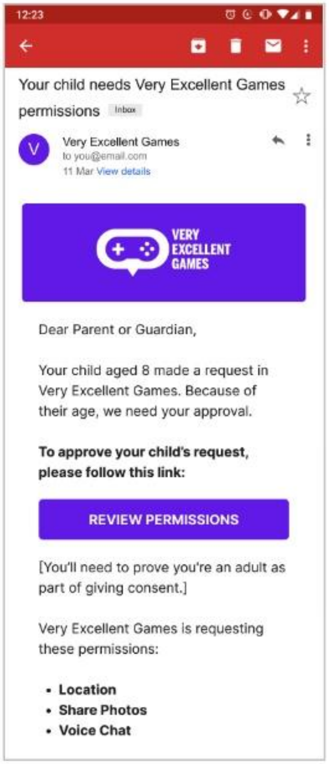
Enter a parent or guardian email address

Due to your age, your account is now a Cabined Account. Some features are unavailable until your parent or guardian gives you permission to use them.

We'll send them an email to let them know about your account and how to give you permission.

Parent or Guardian Email Address *: parent@email.com

Continue
Very Excellent Games Privacy Policy
SUPER AWESOME
SuperAwesome — The Leading Parent Verification and Consent Service
Privacy Policy
Terms of Use
Help
English



Your child needs Very Excellent Games permissions

Very Excellent Games
to you@email.com
11 Mar View details

Dear Parent or Guardian,

Your child aged 8 made a request in Very Excellent Games. Because of their age, we need your approval.

To approve your child's request, please follow this link:

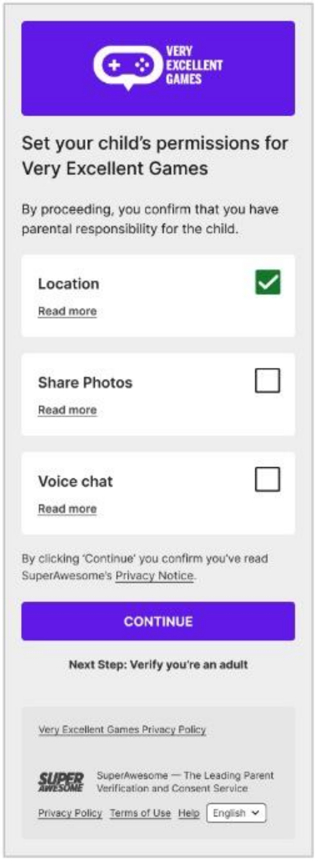
[You'll need to prove you're an adult as part of giving consent.]

Very Excellent Games is requesting these permissions:

- **Location**
- **Share Photos**
- **Voice Chat**

VPC Flow including Facial Age Estimation as PV method

- Parent grants permissions
- Parent chooses a verification method



Set your child's permissions for Very Excellent Games

By proceeding, you confirm that you have parental responsibility for the child.

☑ Location
Read more

□ Share Photos
Read more

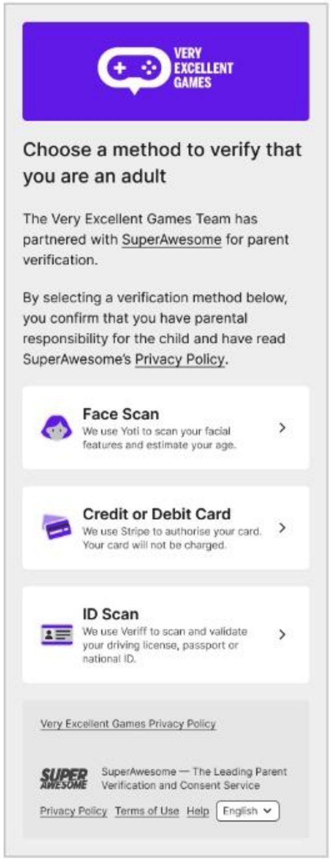
□ Voice chat
Read more

By clicking 'Continue' you confirm you've read SuperAwesome's Privacy Notice.

Next Step: Verify you're an adult

Very Excellent Games Privacy Policy

SuperAwesome — The Leading Parent Verification and Consent Service



Choose a method to verify that you are an adult

The Very Excellent Games Team has partnered with SuperAwesome for parent verification.

By selecting a verification method below, you confirm that you have parental responsibility for the child and have read SuperAwesome's Privacy Policy.

Face Scan — We use Yoti to scan your facial features and estimate your age.

Credit or Debit Card — We use Stripe to authorise your card. Your card will not be charged.

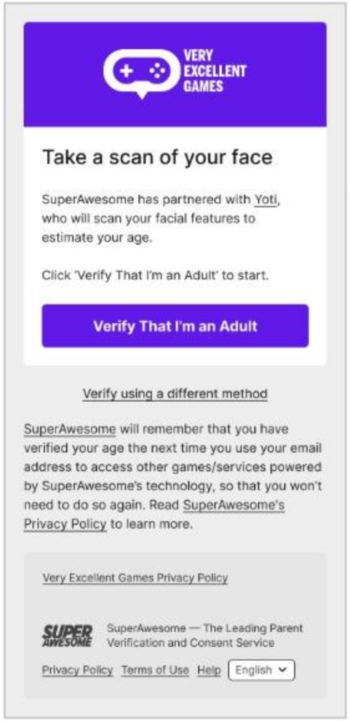
ID Scan — We use Veriff to scan and validate your driving license, passport or national ID.

Very Excellent Games Privacy Policy

SuperAwesome — The Leading Parent Verification and Consent Service

VPC Flow including Facial Age Estimation as PV method

- Parent has selected Face Scan method, and is taken to Yoti's opt-in screen
- Parent is asked for permission to access the camera



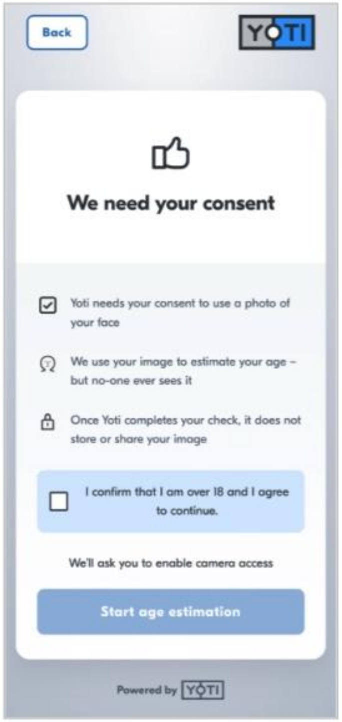
Take a scan of your face

SuperAwesome has partnered with Yoti, who will scan your facial features to estimate your age.

Click 'Verify That I'm an Adult' to start.

SuperAwesome will remember that you have verified your age the next time you use your email address to access other games/services powered by SuperAwesome's technology, so that you won't need to do so again. Read SuperAwesome's Privacy Policy to learn more.

SuperAwesome — The Leading Parent Verification and Consent Service



We need your consent

☑ Yoti needs your consent to use a photo of your face

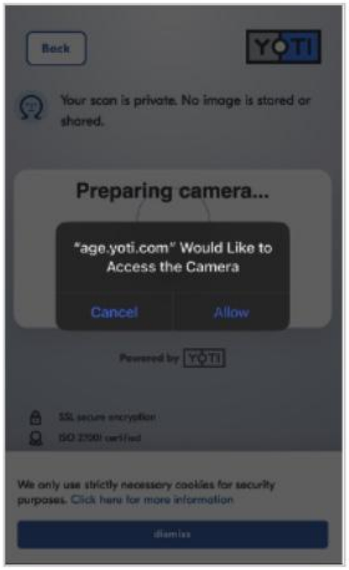
We use your image to estimate your age – but no-one ever sees it

Once Yoti completes your check, it does not store or share your image

☐ I confirm that I am over 18 and I agree to continue.

We'll ask you to enable camera access

Optional opt-in consent screen—configurable by developer



Your scan is private. No image is stored or shared.

Preparing camera...

"age.yoti.com" Would Like to Access the Camera

SSL secure encryption

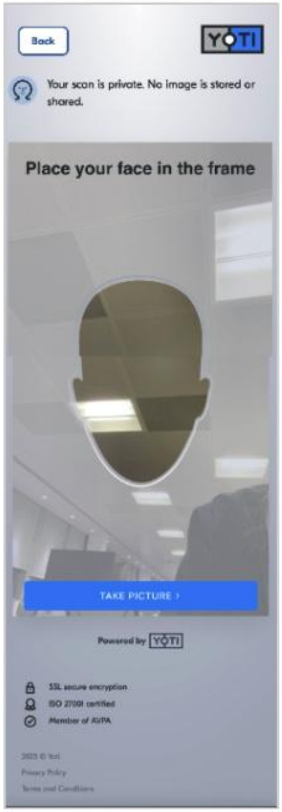
ISO 27001 certified

We only use strictly necessary cookies for security purposes. Click here for more information

VPC Flow including Facial Age Estimation as PV method

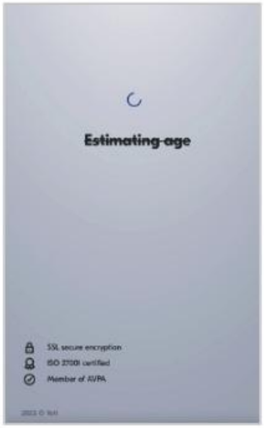
- Parent places face in frame, Yoti checks for liveness and scans the face
- Yoti processes facial scan and deletes the image

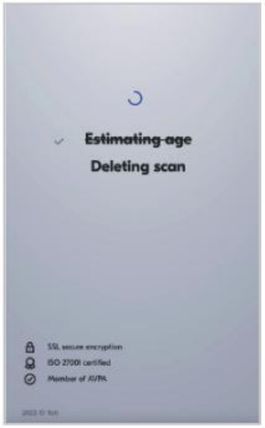
*See slide 6 for an example of what happens if the user fails the liveness test

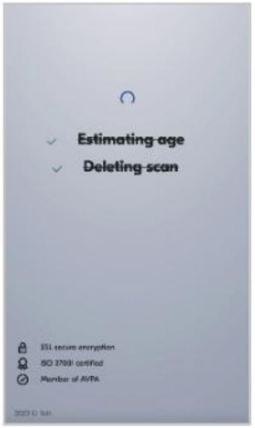


Your scan is private. No image is stored or shared.

Place your face in the frame


~~Estimating age~~

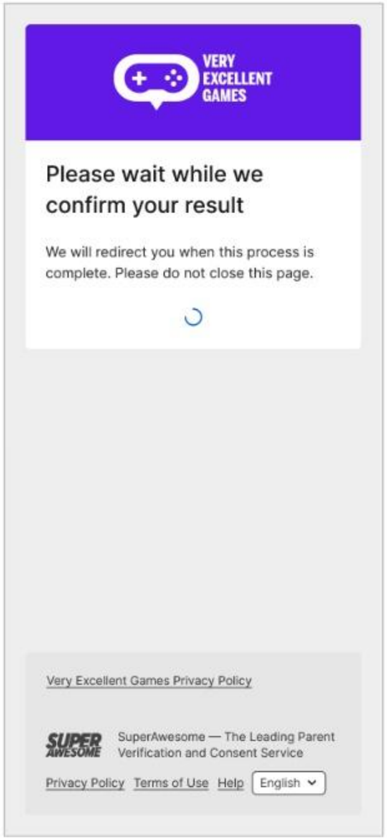

✓ ~~Estimating age~~
Deleting scan


✓ ~~Estimating age~~
✓ ~~Deleting scan~~

VPC Flow including Facial Age Estimation as PV method

- When scan is completed, parent is returned to developer's account setup flow

* See slide 7 for an example of what happens if the user is determined to be below the relevant age threshold

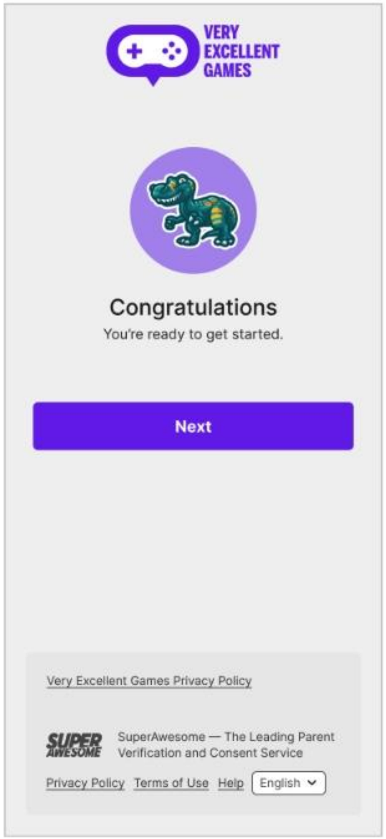


Please wait while we confirm your result

We will redirect you when this process is complete. Please do not close this page.

Very Excellent Games Privacy Policy

SuperAwesome — The Leading Parent Verification and Consent Service



Congratulations

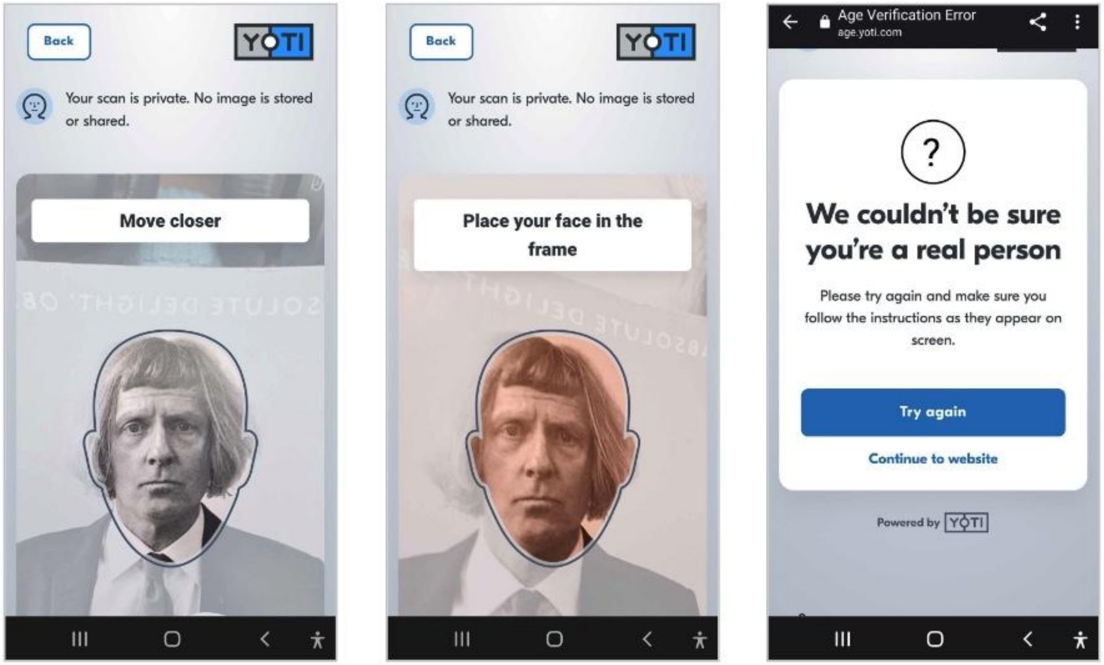
You're ready to get started.

Very Excellent Games Privacy Policy

SuperAwesome — The Leading Parent Verification and Consent Service

VPC Flow including Facial Age Estimation as PV method

- User attempts to use a photo on a book cover and fails liveness test
- Verification fails and user is not permitted to provide permissions for the child



Your scan is private. No image is stored or shared.

Your scan is private. No image is stored or shared.

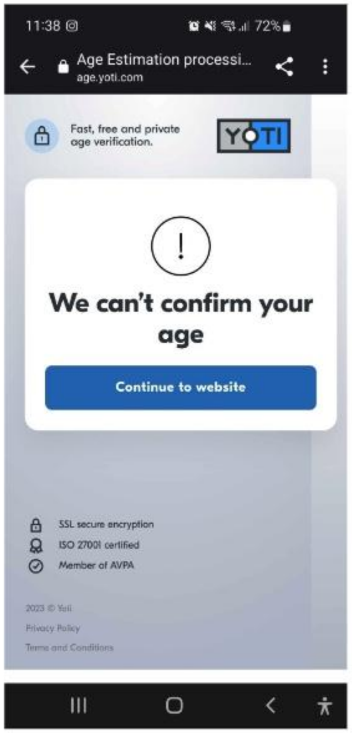
?

We couldn't be sure you're a real person

Please try again and make sure you follow the instructions as they appear on screen.

VPC Flow including Facial Age Estimation as PV method

- User is estimated to be below the threshold age
- Verification fails and user is not permitted to provide permissions for the child



Fast, free and private age verification.

We can't confirm your age

SSL secure encryption

ISO 27001 certified

Member of AVPA

2023 © Yoti

Privacy Policy

Terms and Conditions

APPENDIX C: Evidence of Accuracy, Success Rate, Effectiveness, Fairness and External Validation of Yoti's Facial Age Estimation

The additional information below is sourced from the results of Yoti's extensive testing, as described in its publications, from analysis of live implementations conducted by both Yoti and SuperAwesome, and from third party sources. In this appendix, we analyze Facial Age Estimation as a parent verification method based on:

- *Accuracy*: how good is the underlying technology at estimating age for the purpose of determining that someone is an adult?
- *Success rate*: how well does this method perform technically, i.e., how smooth is the parent experience compared to other methods?
- *Effectiveness*: how good is the VPC method incorporating Facial Age Estimation at separating adults from non-adults?
- *Fairness*: does any bias inherent in the underlying technology materially impact groups of users unfairly?

Accuracy

Facial Age Estimation represents advances in facial analysis technology. This technology has reached a level of accuracy and reliability that makes it as or more reliable as other methods of parent verification currently in use.

Yoti is transparent in describing how Facial Age Estimation was developed and has evolved, through regular publication of detailed white papers since January 2019. In each version, Yoti has published the steadily improving accuracy levels, with measures including mean absolute error rates (MAE), false positives, false negatives for each year of age by gender and skin tone and now also standard deviation.[45]

For the proposed use case – determining whether someone is an adult – the most relevant accuracy metric is the rate of false positives (FPR). FPR indicates what proportion of users that are under 18 are estimated to be adults by the Facial Age Estimation system. In Yoti's implementation (with the pass/fail threshold set at an age of 25), the average FPR is 0.03%. This means that only 3 in 10,000 under-18 users who try to pass themselves off as an adult might get through, which is likely a materially lower false positive rate than other methods, which can be circumvented by the child gaining access to a parent payment card or SSN, for example.

False positive rate (FPR) for 6-17 year-olds at thresholds of 21, 23 and 25

Threshold	Female	Male	Overall
t=21	0.40%	0.40%	0.40%
t=23	0.10%	0.10%	0.10%
t=25	0.04%	0.02%	0.03%

[45] Yoti White Paper, supra n. 4.

Success rate

Facial Age Estimation returns significantly fewer errors or failed transactions than other VPC methods. It is also more successful in identifying attempts to cheat the system, for example by underage users attempting to verify by using a photograph of an adult, or by asking an older sibling to pretend to be the parent.

In terms of technical success rate, i.e., the percentage of attempts to use the verification method that leads to a valid result,[46] Facial Age Estimation fares significantly better than other methods of verification, with a 97% success rate. This addresses one of the biggest known problems of other commonly used parent verification methods – payment card, Social Security Number ("SSN"), or scans of identity documents ("ID Scan"). Based on recent KWS data,[47] the percent of verification attempts using these methods that result in failure, i.e., no useable result is:

● Payment card:	35%
● Social security number:	34%
● Identity document scan:	50%

This leads to frustration among parents and is the source of a large proportion of customer service complaints received by developers.[48] In the case of Facial Age Estimation, a scan may fail due to a poor quality submission, for example because the camera was blocked or the lens smudged, the lighting was insufficient to generate a clear image, or a very old device was used. This occurs on average 3% or less of the time.

A Facial Age Estimation scan may be technically successful, but still deliver a negative outcome (no age estimation). This can occur if the user fails the liveness test, in other words the system believes that it is being shown a static image rather than an actual person. While this is characterized as a rejection in the system, it may in fact be a successful scan that has removed from the flow an attempt to cheat it (or "spoof" it, in the tech vernacular).[49] This occurs on average 6-7% of the time.

Effectiveness

Finally, the evidence supports that Facial Age Estimation is effective in ensuring only adults are able to complete the VPC process. In the Applicants' (and the proposed) implementation, the acceptance threshold is set to an age of 25 in order to minimize the risk of false positives (i.e., minors being estimated to be adults). Based on three months of parent verifications conducted by the Applicants until 30 April in the U.K. and in those European countries where the age of digital

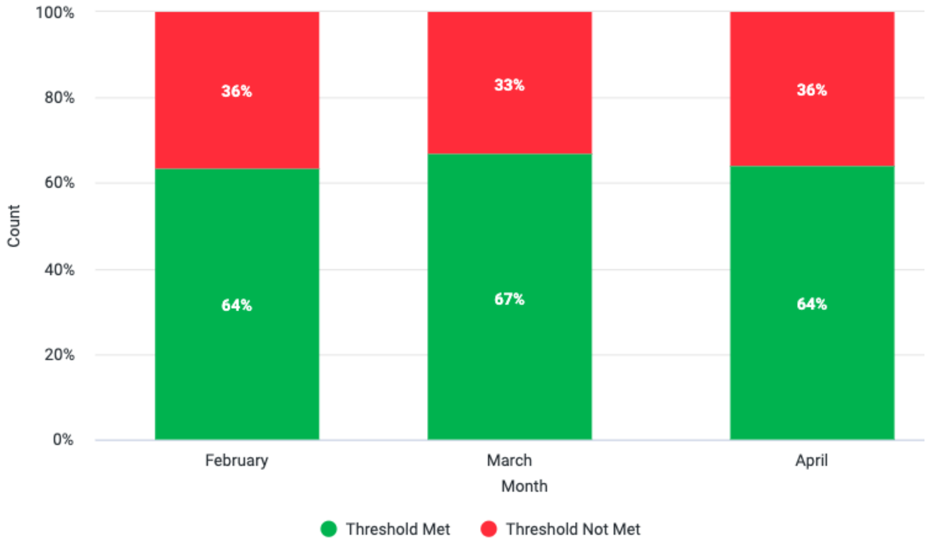
[46] There are three possible valid results: (1) Yes, this person is an adult; (2) No, this person is not an adult; (3) This is not a person. See *Appendix B, Example of Implementation of Facial Age Estimation for VPC*, for screenshots of these different results.

[47] Based on 2.1 million parent verifications performed worldwide by KWS between February 2 and April 30, 2023.

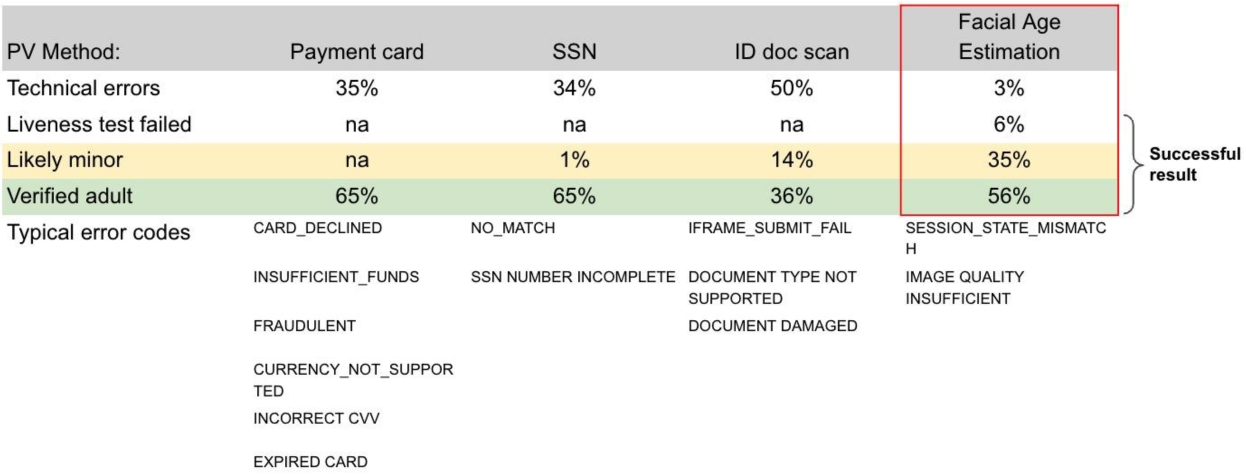
[48] Based on review of the types of customer service calls received by SuperAwesome and by Epic Games during 2022 and 2023.

[49] *See* Yoti White Paper for more information about how its anti-spoofing technology works, https://www.yoti.com/wp-content/uploads/Yoti-MyFace-Liveness-White-Paper-March-2023.pdf.

consent is 13,[50] 33-36% of age estimations identified that the person is not an adult, but rather a child or teen trying to circumvent the verification step. In this case, the verification is denied, and the user is prevented from providing consent for the minor. If the user believes this is an error (i.e., they are in fact a parent whom the system has estimated to be below 25 years old), they can go back in the process and verify their age using another method.



Seen in the context of the age distribution spectrum, it is clear that Facial Age Estimation is highly effective in preventing children from falsely providing parental consent. To summarize, the below table provides a side-by-side comparison of the success rate and effectiveness of the various parent verification methods used by KWS in 2023:[51]



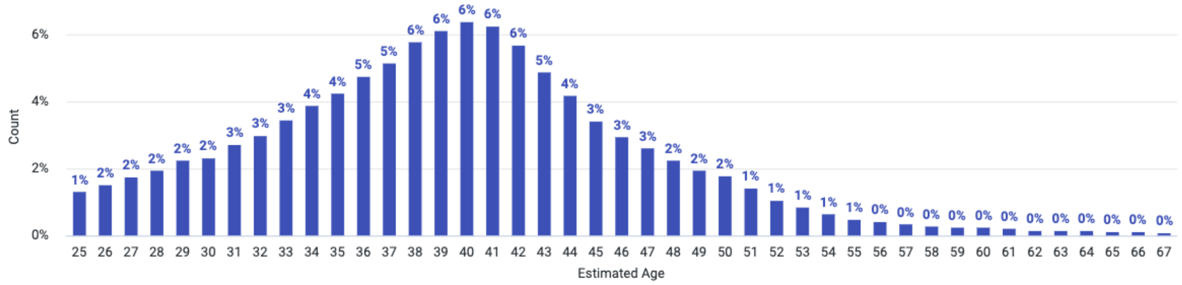
PV Method:	Payment card	SSN	ID doc scan	Facial Age Estimation	
Technical errors	35%	34%	50%	3%	
Liveness test failed	na	na	na	6%	Successful result
Likely minor	na	1%	14%	35%	
Verified adult	65%	65%	36%	56%	
Typical error codes	CARD_DECLINED INSUFFICIENT_FUNDS FRAUDULENT CURRENCY_NOT_SUPPOR TED INCORRECT CVV EXPIRED CARD	NO_MATCH SSN NUMBER INCOMPLETE	IFRAME_SUBMIT_FAIL DOCUMENT TYPE NOT SUPPORTED DOCUMENT DAMAGED	SESSION_STATE_MISMATC H IMAGE QUALITY INSUFFICIENT	

Based on the distribution of estimated ages detected by the Facial Age Estimation system, we can assess both the effectiveness of the system and draw some conclusions about user (including child) behaviors.

[50] Belgium, Sweden, Denmark, Estonia, Finland, Latvia, Portugal and Malta.

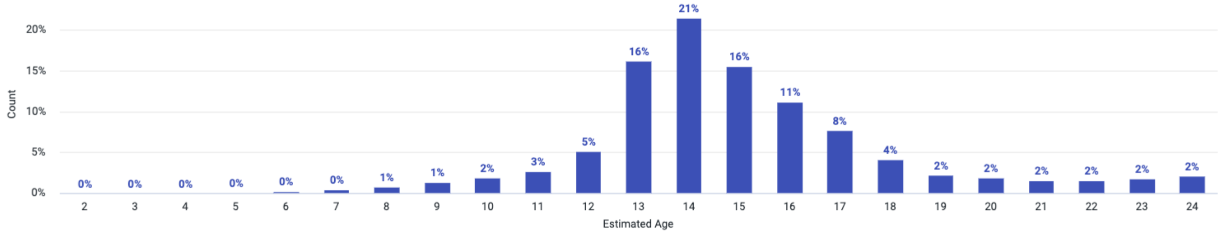
[51] Based on 2.1 million parent verifications performed worldwide by KWS between February 2 and April 30, 2023.

Below is the distribution of adult ages estimated in the Applicants' implementation in the U.K. and European countries where the age of digital consent is 13:[52]



It shows that the bulk of parents of children requesting parental consent are between 35 and 43. This would correlate with an expected average age of parents at the time of first birth of 29 for mothers and 31 for fathers. The average age of parents having kids age 6 and older is 35.[53]

Below is the distribution ages estimated which fell below the threshold of 25, i.e., they were prevented from providing consent:[54]



This data suggests that a significant number of children are asking their 13+ siblings or friends (including young adults) to verify on their behalf.

Assessing False Negatives

Finally, it is important to understand the impact of false rejection of adults, i.e., the likelihood that a legitimate parent over 25 is estimated by the system to be under 25 and hence rejected. The True Positive Rate (TPR) is a measure of the likelihood that an adult of age over 25 will be correctly estimated by the system to be an adult. Using TPR, we can compute its opposite, the False Negative Rate (FNR), i.e., the likelihood that a legitimate parent over 25 is estimated by the system to be under 25 and hence rejected. We then apply a weighting to the FNR that reflects the distribution of ages of people that have gone through facial age estimation via KWS to obtain the weighted FNR (wFNR). The Applicants' implementation – with the pass/fail threshold set at

[52] Data from facial age estimations conducted by Yoti for KWS in the UK. and those EU countries where the age of digital consent is 13, between February 11 and May 1, 2023.

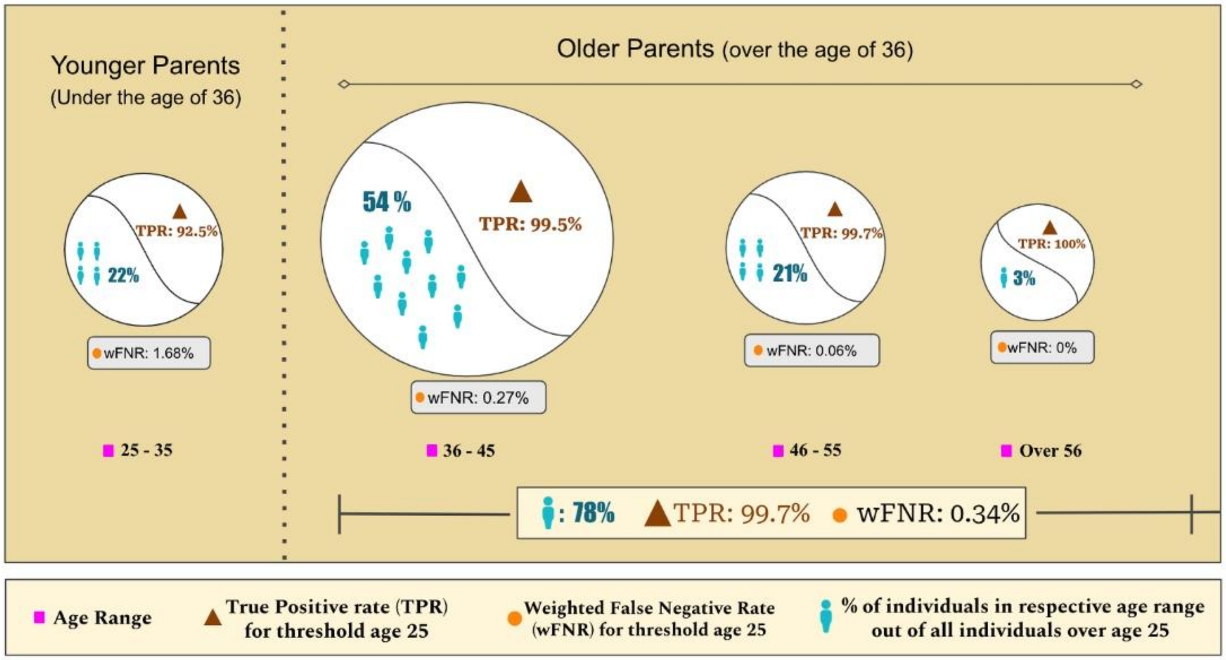
[53] Osterman MJK et al., NATIONAL VITAL STATISTICS REPORTS, VOL. 72, NO 1, at *Figure 2. Birth rates, by selected age of mother: United States, 1990-2021* (Jan. 31, 2023), https://www.cdc.gov/nchs/data/nvsr/nvsr72/nvsr72-01.pdf

[54] Data from facial age estimations conducted by Yoti for KWS in the UK and those EU countries where the age of digital consent is 13, between February 11 and May 1, 2023.

25 – specifically prioritizes minimizing the False Positive Rate (to prevent kids or teens spoofing the system) over wFNR (since wrongly rejected adults can go back and verify their age using another method). Nonetheless, it's worth noting that in practice the wFNR rate is low.

For those over 36, the TPR is 99.7% and the wFNR is 0.34%, which means that for every 10,000 adults over 36, 34 might be rejected because the system thinks they are under 25. For younger parents, i.e., those between 25 and 35, the TPR is 92.5% and so the wFNR is higher, at 1.68%, which means that for every 10,000 adults between 25 and 36, 168 might be rejected because the system thinks they are under 25.

TPR and wFNR to understand proportion of individuals over 25 who are correctly accepted and those falsely rejected



**wFNR above is calculated as: [(sum of individuals in the age range/sum of all individuals above 25)*(1-TPR)]*

Those that are in the 'buffer' zone of 18-24, which currently represent about 5% of age estimations, will be rejected by the system in its current configuration. Based on U.S. birth data (covering birth rates for women aged 18 or under who have given birth between 2011-2017 and thus have a child in 2023 between 6-12 years), we can estimate that 2.74% of 18-24-year-old women are parents[55]. Combining this with the proportion of age estimations that are in the range 18-24, we estimate that the probability of incorrect rejections for a parent due to them being in this 'buffer' age range is about 0.11%.[56] This also suggests that most individuals identified in this age group are older siblings or other adults attempting to trick the system. Those individuals that

[55] Based on birth rates for women aged 18 or under between 2011-2017. CDC, Nat'l Ctr. for Health Stat., *About Natality, 2007-2021 Results* (last accessed May 4, 2023), https://wonder.cdc.gov/natality-current.html.

[56] Factoring in 5% age estimations between 18-24 observed for KWS in Yoti's stats and 81.9% TPR observed for 18-24 age group in Yogi's Age Estimation model, version: March 2023.

are rejected and who are genuine parents can go back in the process and verify their age using another method.

Fairness

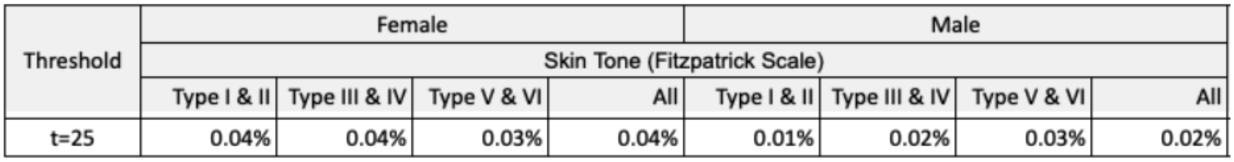
Fairness is a key area of concern for providers of facial age estimation.

Yoti has taken several steps to mitigate bias by collecting, with full informed consent, training data on a diverse set of ages and range of skin tones, with consideration of gender balance. In addition to building the training data set from Yoti users from 190 countries, Yoti has specifically gathered additional age verified images in South Africa,, Kenya, Russia, Mexico, India and other Asian countries as a way of ensuring that the dataset was as diverse as possible and therefore mitigating the likelihood of bias.

Yoti's white paper presents the mean absolute error (MAE) in facial age estimation across six classes: female (for three different skin tones), and male (for three different skin tones). For skin tone, Yoti uses the widely used Fitzpatrick dermatological scale,[57] which describes six bands, from Type I (lightest) to Type VI (darkest). Yoti's analysis presents data in three bands (based on Fitzpatrick Types I & II, Types III & IV, and Types V & VI).[58]

For the Applicants' proposed use case of parent verification, the FPR difference (i.e., the likelihood of an under-18-year-old being verified as an adult) between male and female users is 2 out of 10,000 versus 4 out of 10,000 respectively. The FPR differences among a range of skin tones is between 1 in 10,000 to 4 in 10,000. Across skin tones and gender, the FPR remains consistently well below 0.1%, which suggests any impact from bias is immaterial to the use case:[59]

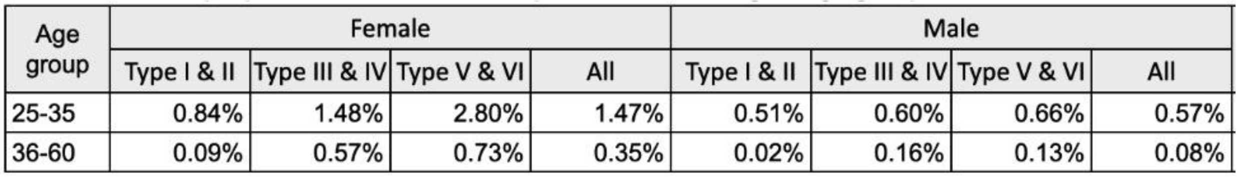
False positive rate (FPR) for 6-17 year-olds at an age threshold of 25, by skin tone and gender (ave = 0.03%)



Threshold	Female				Male			
	Skin Tone (Fitzpatrick Scale)							
	Type I & II	Type III & IV	Type V & VI	All	Type I & II	Type III & IV	Type V & VI	All
t=25	0.04%	0.04%	0.03%	0.04%	0.01%	0.02%	0.03%	0.02%

If we look at the weighted False Negative Rate (wFNR) we can see a similar pattern, i.e., that the difference in rejection rates between gender and skin tone is very small:[60]

Weighted false negative rate (wFNR) based on proportion of individuals impacted considering all ages



Age group	Female				Male			
	Type I & II	Type III & IV	Type V & VI	All	Type I & II	Type III & IV	Type V & VI	All
25-35	0.84%	1.48%	2.80%	1.47%	0.51%	0.60%	0.66%	0.57%
36-60	0.09%	0.57%	0.73%	0.35%	0.02%	0.16%	0.13%	0.08%

[58] For more on Yoti's work on reducing bias in age estimation, *see* Yoti White Paper, supra n. 4 at 4, 30.

[59] Yoti data; FPRs are based on performance of Yoti's Age Estimation model, version: March 2023.

[60] Yoti data; wFNRs are based on performance of Yoti's Age Estimation model, version: March 2023 combined with KWS age distribution observed in 307,883 checks across all age groups from 13 Feb. 2023 to 17 Apr. 2023 in the UK and EU countries.

The data suggests that for those between 25 and 35, 15 out of 1,000 females vs 7 out of 1,000 males might be incorrectly classified as under-25 (and would have the option of verifying using another method). The range of difference by skin tone is between 8 out of 1,000 vs 28 out of 1,000. While bias exists, as is inherent in any automated system, this is not material, especially as compared to the benefits and the increase in access to certain groups of parents (as outlined in Appendix D).

External Validation

In recent years, facial age estimation technology has been deployed or tested for various age assurance applications beyond parent verification, such as the purchase of age-restricted goods in a physical environment,[61] and the gating of age-restricted online services.[62] In November 2022, for example, social media platform Instagram rolled out age assurance using facial age estimation in order to check that users are the age they claim to be when trying to change the age on their social media account.[63] Similarly, Facebook announced it would use facial age estimation to prevent users under 18 years old from accessing its Facebook Dating service.[64] This broad adoption can be attributed to the advances in technology rapidly increasing effectiveness of age estimation without the need for facial recognition/identification of individuals.

Yoti's Privacy-Protective Facial Age Estimation has been externally tested and certified by the U.K. Age Check Certification Scheme ("ACCS"), an accredited certification body that independently certifies online and offline age assurance systems.[65] In its certification report, which tested the use case of verifying that someone is an adult, the ACCS stated that "The Yoti AI Services Age API version 1.1.1. . .assessed on or before 17th November 2020 can be stated to accurately estimate the age of person of nominal age 18 as being under the age of 25 with 98.89% reliability where results are stated by the Yoti system to an uncertainty of less than 4.6

[61] In December 2022, the U.K. Home Office published the results from trials it conducted of various age verification and age estimation technologies to prevent minors from purchasing age-restricted products at supermarket checkouts. During the trial, no underage customers purchased age restricted items when using the new Yoti age verification technology. The Home Office concluded that "[u]ptake of age estimation technology at self-scan checkouts suggests that there is appetite for digital age assessment." Office for Product and Standards, U.K. Home Office, *Key learning from the trial* (Dec. 30, 2022), https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox/key-learning-from-the-trial.

[62] Regulated industries, such as online gambling in the U.K., have been early adopters. See Bacta to integrate latest age estimation technology in YALP app, European Gaming (Nov. 18, 2019), https://europeangaming.eu/portal/press-releases/2019/11/18/58721/bacta-to-integrate-latest-age-estimation-technology-in-yalp-app/.

[63] Ryan Morrison, *Instagram rolls out age verification for UK users*, TECH MONITOR (Nov. 7, 2022), https://techmonitor.ai/technology/ai-and-automation/instagram-age-verification-uk.

[64] Erica Finkle, *Bringing Age Verification to Facebook Dating*, META NEWSROOM (Dec. 5, 2022), https://about.fb.com/news/2022/12/facebook-dating-age-verification/.

[65] The ACCS has tested the viability, accuracy and reliability of Yoti's technology for digital identity verification and age estimation. See the Yoti registry entry on the ACCS site: https://www.accscheme.com/registry/yoti-ltd.
The ESRB has an arrangement with the ACCS, whereby ESRB member companies can receive a discount on the ACCS's certification services for its ICO-authorized Age Appropriate Design Code Certification Scheme.

years."[66] This rate of reliability has since improved to 99.97%, as independently verified by ACCS in their review of Yoti's white paper.[67]

Regulators have also approved of facial age estimation technology, in privacy and data protection and other regulatory contexts. In 2022, the French data protection regulator, the Commission Nationale de l'Informatique et des Libertés ("CNIL"), published an analysis of age verification methods in the context of keeping minors out of adult services, concluding that "The analysis of facial features by an automatic system accessing the computer's webcam, without biometric facial recognition, makes it possible to block access for the youngest and to authorize access for people who are well over 18 years old" (English translation).[68] And so although the report was not supportive of age *verification* using existing methods for *younger users*, the CNIL noted a distinction between that and age *estimation* for *older users*. It revisited this study, more recently, in a February 2023 blog post, where it re-emphasized that "it considers acceptable the use of age verification by validation of a payment card or a process of *facial age estimation based on facial analysis without facial recognition*" (emphasis added) (English translation).[69]

Similarly, the U.K. Information Commissioner ("ICO") published a report in October 2021 favorably reviewing age assurance methods companies can use to comply with the Age Appropriate Design Code ("AADC"). It stated that "[a]ge estimation based on biometrics, such as facial or hand geometry, has the potential to be more privacy friendly if data minimisation and purpose limitation are applied rigorously."[70] That same year, the ICO conducted a voluntary audit of Yoti's app, and concluded that Yoti's approach is consistent with the requirements of the GDPR and AADC.[71]

In November 2022, the international non-profit Family Online Safety Institute ("FOSI") published the results of its cross-jurisdictional survey of the awareness, attitudes, and behaviors of both parents and children regarding age assurance methods. In analyzing the data, FOSI

[66] ACCS, *Yoti Ltd - Age Estimation Technologies,* https://www.accscheme.com/registry/yoti-ltd. *See also Appendix C, Accuracy* for more data on the accuracy of Yoti's age estimations in the context of verifying adults.

[67] Yoti's 2022 white paper was independently verified by the ACCS as to the measurement methodology and accuracy of Yoti's results: "The training, testing and results reporting presented in the Yoti white paper have been independently validated by ACCS, who have certified that Yoti have deployed appropriate methodologies to analyze the performance of their Facial Age Estimation algorithm, including ensuring appropriate separation of machine learning training data, testing data and validation data." Yoti White Paper, supra n. 4 at 24.

[68] CNIL, *Contrôle de l'âge sur les sites web : la CNIL invite à développer des solutions plus efficaces et respectueuses de la vie privée* (July 26, 2022), https://www.cnil.fr/fr/controle-de-lage-sur-les-sites-web-la-cnil-invite-developper-des-solutions-plus-efficaces-et.

[69] CNIL, *Contrôle de l'âge pour l'accès aux sites pornographiques* (Feb. 21, 2023), https://www.cnil.fr/fr/controle-de-lage-pour-lacces-aux-sites-pornographiques.

[70] ICO, *Information Commissioner's opinion: Age Assurance for the Children's Code* (Oct. 14, 2021), https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf.

[71] In its final report, the ICO stated: "There is a high level of assurance that processes and procedures are in place, that the organisation is in conformance with the AADC and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-conformance with AADC and data protection legislation." *See* ICO, *Yoti: Age Appropriate Design Code Audit Report* 5 (Dec. 2021), https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019830/age-appropriate-design-code-yoti-app-audit-report-executive-summary-v1_0.pdf.

concluded that "Anonymity [is] key to privacy for parents," and acknowledged facial age estimation as a positive development to meet this preference.[72]

[72] FOSI, *Making Sense of Age Assurance: Enabling Safer Online Experiences* (Nov. 14, 2021), https://global-uploads.webflow.com/5f47b99bcd1b0e76b7a78b88/636d13257232675672619f45_MAKING%20SENSE%20OF%20AGE%20ASSURANCE%20FULL%20REPORT%20-%20FOSI%202022_compressed.pdf ("Many parents link anonymity to their idea of online privacy, which was most pronounced in France, followed by the US and UK []. This focus on anonymity could be a positive indicator for the continued rise of age assurance methods such as age estimation, where for example, facial features are scanned for accuracy within an age range, *without a connection* to identity or personal information.") (Emphasis in original).

APPENDIX D: The Benefits of Facial Age Estimation in Terms of Parent Access and Choice

Facial Age Estimation does not require ownership of a government-issued identity document or access to payment methods such as credit cards. It therefore promotes inclusion by enabling age verification for people who do not have the necessary credentials under the most common methods of VPC authorized by the COPPA Rule. In the United States, an estimated 4.5% of households (approximately 5.9 million) were "unbanked" in 2021 and 17% do not have a credit card.[73] About 15.9% of eligible Americans do not have a valid driver's license,[74] and there is a strong correlation between lower-income and minority ethnic groups and low rates of photo ID ownership.[75]

The proposed implementation presents Facial Age Estimation alongside other methods, in order for parents to choose the method that works best for them. The Applicants' experience of operating Facial Age Estimation for legally required parental consent outside the U.S. shows that when parents are offered several methods to verify that they are adults, Facial Age Estimation is often the preferred choice (and in some cases overwhelmingly so), with between 50% and 80% of parents choosing it over other methods (depending on the country and other methods offered).[76]

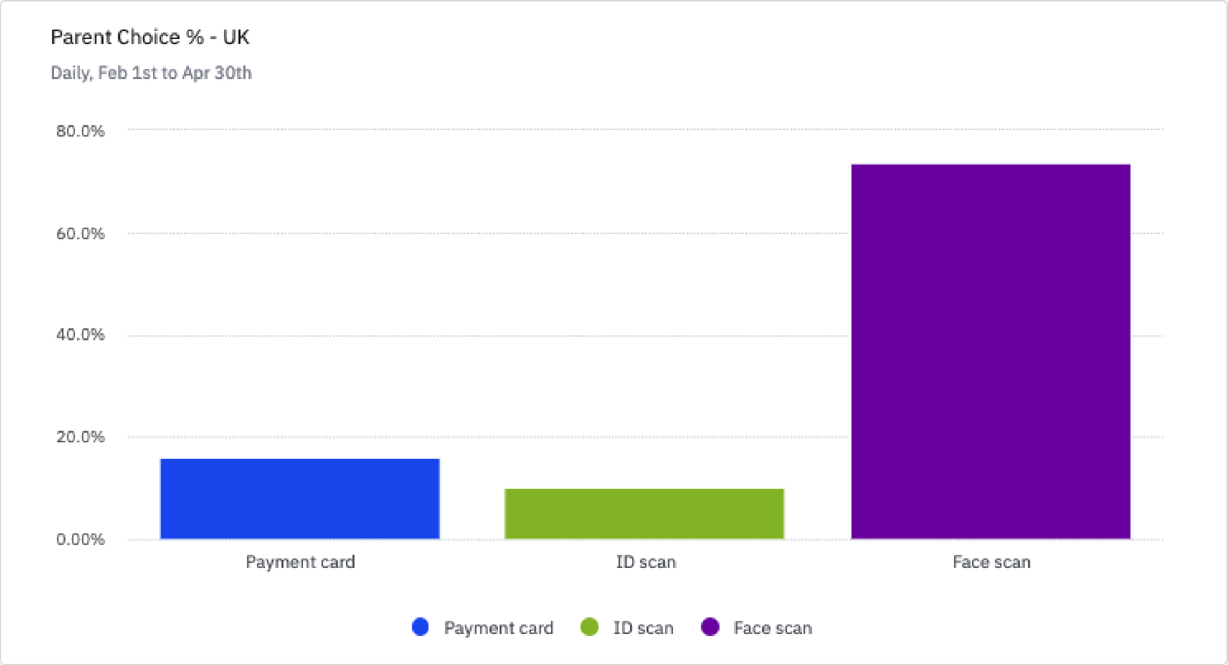
Below are illustrations of data from KWS regarding the choice parents make when presented with various methods of parent verification in different countries. Note that the only instance when Facial Age Estimation is not the preferred method is when the alternative is a widely used domestic identity number, such as the Cadastro de Pessoas Físicas, or CPF, in Brazil.

[73] Board of Governors of the Fed. Reserve Sys., *Economic Well-Being of U.S. Households in 2020 - May 2021: Banking and Credit* (last updated June 13, 2022), https://www.federalreserve.gov/publications/2021-economic-well-being-of-us-households-in-2020-banking-and-credit.htm

[74] Hedges & Company, *How Many Licensed Drivers are There In The Us?* (last visited Apr. 25, 2023), https://hedgescompany.com/blog/2018/10/number-of-licensed-drivers-usa/#:~:text=60.1%25-,Percentage%20of%20adults%20without%20a%20driver's%20license,20%20to%2024%20(19.2%25).

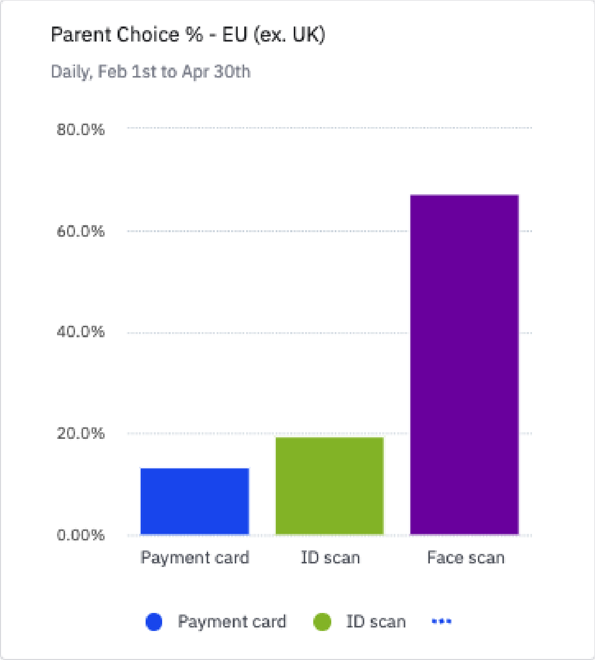
[75] According to Project Vote research, "Thirteen percent of Blacks, 10 percent of Hispanics, but only 5 percent of Whites lack photographic identification. [...] Lower-income individuals are less likely to have photo ID. Twelve percent of adults living in a household with less than $25,000 annual income lack photo ID, compared to just 2 percent in households with over $150,000 annual income." Research Memorandum by Vanessa M. Perez, on *AMERICANS WITH PHOTO ID: A Breakdown of Demographic Characteristics 1* (Feb. 2015), (on file with Project Vote), https://www.projectvote.org/wp-content/uploads/2015/06/AMERICANS-WITH-PHOTO-ID-Research-Memo-February-2015.pdf.

[76] In its trials, Meta group company Facebook also found that 81% of users who are given a range of options to estimate or verify their age choose facial age estimation. Erica Finkle, Director, *Bringing Age Verification to Facebook Dating*, Meta (Dec. 5, 2022), https://about.fb.com/news/2022/12/facebook-dating-age-verification/.



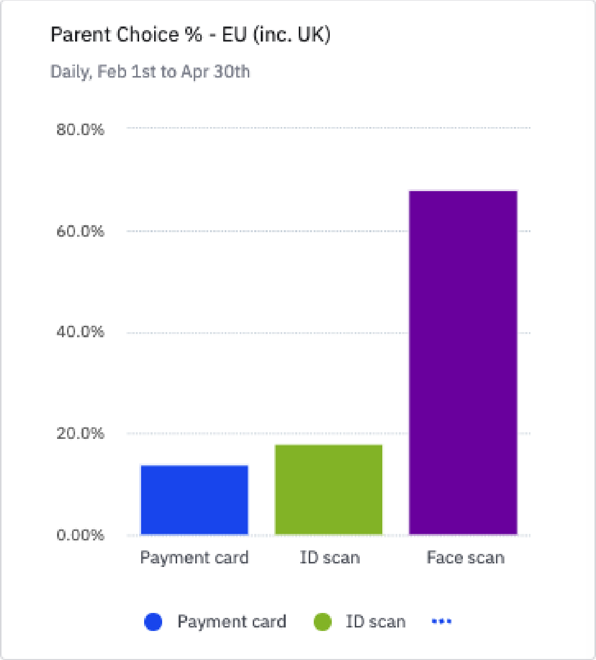
Parent Choice % - UK

Daily, Feb 1st to Apr 30th



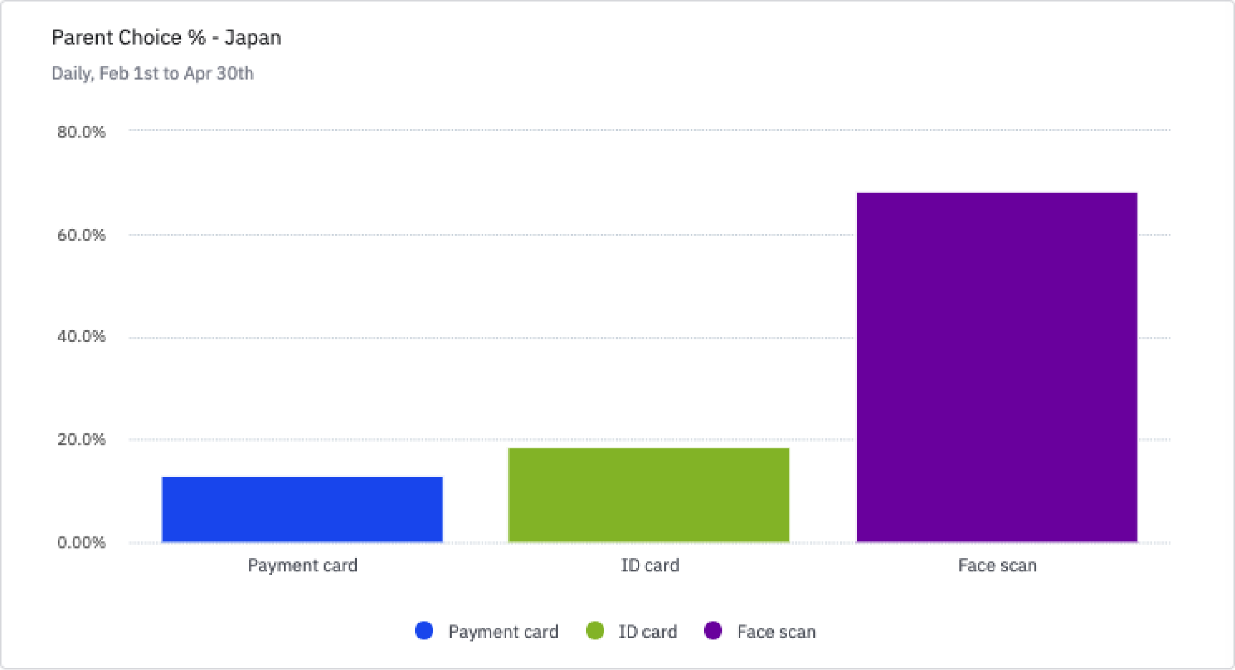
Parent Choice % - EU (ex. UK)

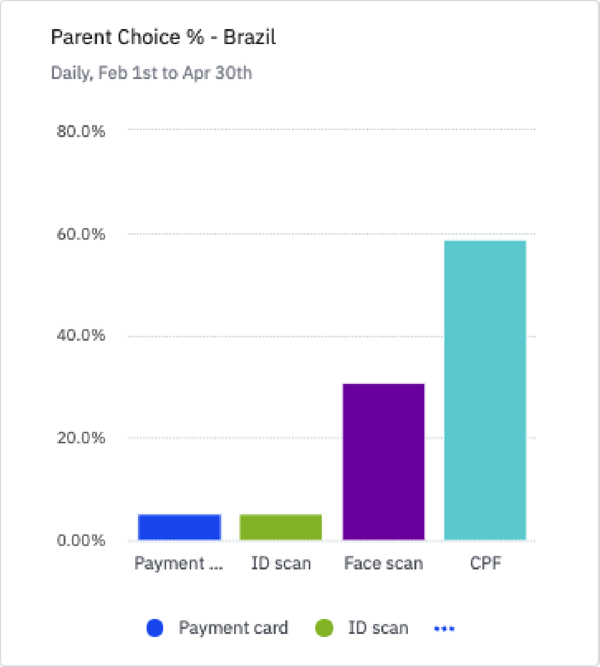
Daily, Feb 1st to Apr 30th

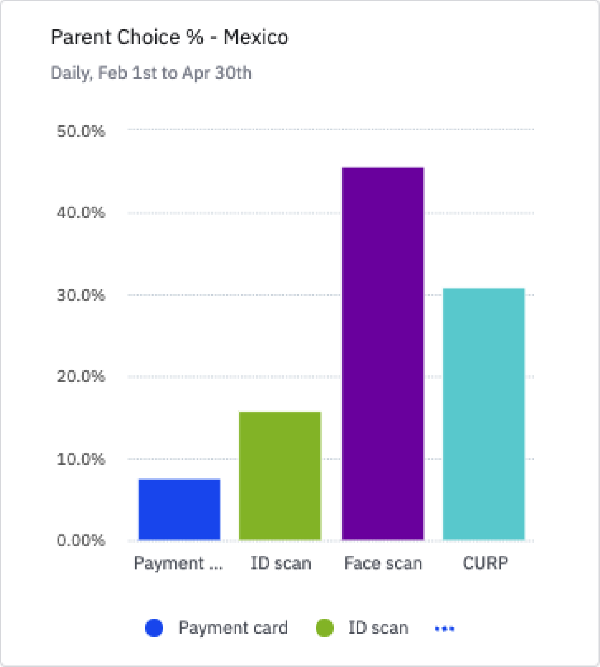


Parent Choice % - EU (inc. UK)

Daily, Feb 1st to Apr 30th

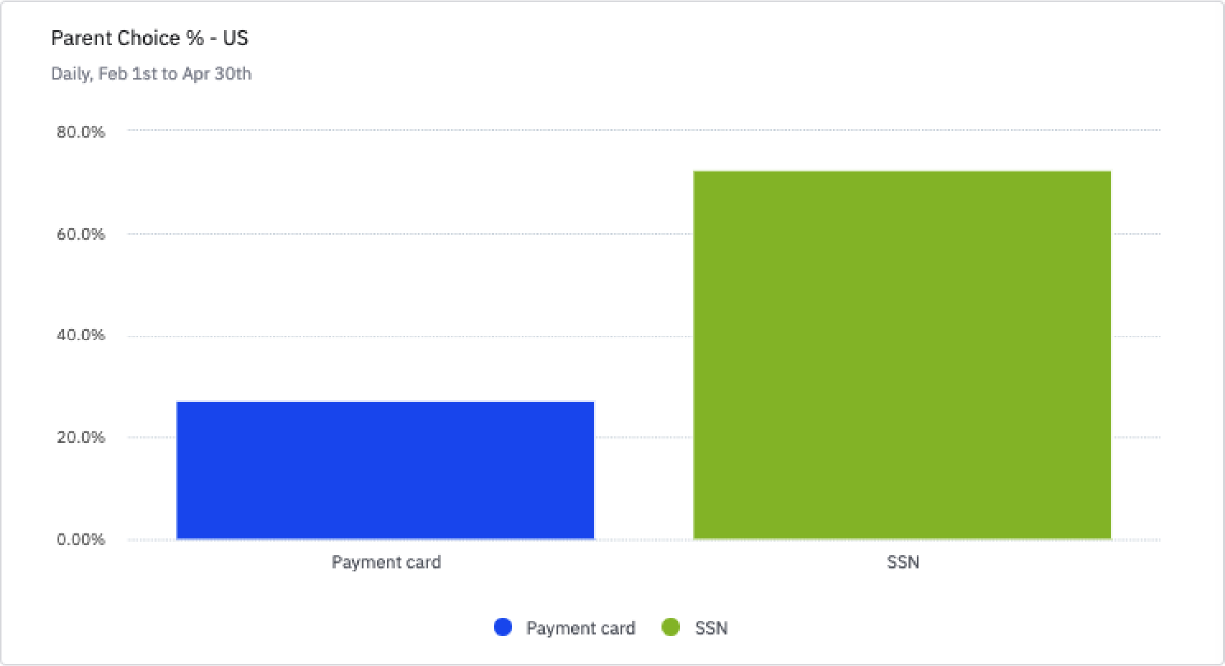






For reference, the current preference of U.S. parents going through the KWS VPC flow, who are given the choice of using either payment card or providing the last 4 digits of their SSN is decidedly in favor of SSN[77]:

[77] Based on 2.1 million parent verifications performed by KWS in the U.S. between February 2 and April 30, 2023.


Parent Choice % - US
Daily, Feb 1st to Apr 30th
80.0%
60.0%
40.0%
20.0%
0.00%
Payment card
SSN
● Payment card
● SSN