United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Federal Trade Commission
Office of the Secretary

Riyo submitted a proposed VPC method for approval on July 1, 2015. The Commission published the application in the Federal Register on August 7, 2015.[3] The public comment period closed on September 14, 2015.[4] The Commission received four comments regarding Riyo's application.[5]

The proposed method involves "Face Match to Verified Photo Identification" ("FMVPI"), which combines photo verification identification with facial recognition technology via web and mobile devices. The proposed method involves a two-step process. The first step of FMVPI includes photo identification verification. The parent captures the image of his or her photo identification (e.g. driver's license or passport) with a phone's camera or a webcam. The authenticity and legitimacy of the identification document is then verified using computer vision technology, algorithms, and image forensics to analyze the fonts, holograms, microprint, and other details coded in the document to ensure that the photo identification is an authentic government-issued identification.

The second step of FMVPI involves facial recognition technology. After the photo identification document is authenticated, the system prompts the parent to take a photo of his or her own face with a phone camera or webcam. The system detects facial movements to ensure this photo is of a live person, rather than a photo of a photo. The image of the parent's face is tnton

After careful consideration of the application and the public comments that were submitted in this matter, the Commission has determined that the proposed FMVPI method satisfies Section 312.5(b)(1) of the Rule. Specifically, evidence demonstrates that, like the other approved VPC methods, a method that involves verifying a government-issued identification and then matching the image on that identification with the captured face of a live person can be "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent" as required by the Rule.

Facial recognition technology is now being used to verify identity in a number of settings. For instance, retailers, financial institutions, and technology companies use facial recognition technology for safety and security purposes.[7] While facial recognition technology is not perfect, in recent years, facial recognition technology has rapidly improved in performance, and now can surpass human performance under some conditions.[8] Moreover, the proposed method involves one-to-one verification – comparing one image with a second image – which can be very accurate, in comparison to matching one image with thousands or millions of other images.[9] Moreover, the proposed method also entails review of the two images by trained personnel. In short, identity verification via facial recognition technology can be reasonably reliable for purposes of determining whether an individual pictured in a government-issued identification is the same person in the second image.

We received four public comments on the proposed method. The Center for Digital Democracy's ("CDD") comment raises several concerns. First, CDD questions the efficacy of facial recognition technology as a VPC method on the basis that it has not proven to be accurate or reliable.[10] As noted above, however, facial recognition technology is being used today in a variety of settings that require a significant level of reliability and accuracy. We believe that this technology is sufficiently accurate to accomplish the type of one-to-one matching required in this setting, particularly given that this matching is also reviewed by trained individuals. Our approval of this method rests on the one-to-one matching; we do not opine on any facial recognition method that involves checking a single photo against a database of many photos.

[7] *See, e.g*, U.S. Government Accountability Office, Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law, July 2015 ("GAO Report"), at 8-9. For example, the Orlando International Airport has added facial recognition to its automated passport kiosks, which compare the traveler's face with the biometric information in their e-passport. *See* https://orlando.interplex.net/blog/orlando-airport-first-to-add-facial-recognition/. *See also* Riyo VPC Application, Appendix 1 (indicating that the Jumio facial recognition technology is being used by financial institutions, airlines, and other companies).

[8] *See* GAO Report, at p. 5, *citing* Alice J. O'Toole, P. Jonathon Phillips, Fang Jiang, Janet Ayyad, Nils Penard, and Herve Abdi, *Face Recognition Algorithms Surpass Humans Matching Faces over Changes in Illumination*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(9), 1642-1646 (September 2007), accessed April 24, 2015, http://www.utdallas.edu/~herve/Abdi-opjapa2007.pdf. *See also* National Institute of Standards and Technology, *Face Recognition Vendor Test: Performance of Face Identification Algorithms*, NIST Interagency Report 8009 (Gaithersburg, Md.: May 26, 2014).

[9] *See, e.g.*, http://jain.egr.msu.edu/face-recognition/ (indicating accuracy rate of up to 99%).

[10] *See* CDD's Comments at p. 3, *citing* Patrick Grother & Mei Ngan, *Face Recognition Vendor Test*, *Performance of Face Identification Algorithms*, May 2014. We note that this test focused on one-to-many, and not one-to-one, applications of facial recognition technology.

COPPA, including those that require that operators provide a valid notice prior to collecting personal information and enable parents to exercise their rights to review or delete information collected from their children.[19]

Therefore, the Commission approves the use of facial recognition technology as a VPC method under COPPA, provided it is appropriately implemented as set forth above.

By direction of the Commission.

Donald S. Clark
Secretary

[19] 16 C.F.R. § 312.4; 16 C.F.R. § 312.6.