Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)	
	)	
Jest8 Limited (Trading as Riyo)	)	P–155405
Application for Parental Consent Method	)	

COMMENTS OF CENTER FOR DIGITAL DEMOCRACY

The Center for Digital Democracy ("CDD") respectfully submits these comments in response to *Jest8 Limited, Trading as Riyo, Application for Approval of Parental Consent Method*.[1] CDD is a national nonprofit, nonpartisan organization dedicated to promoting responsible use of new digital communications technologies, especially on behalf of children and their families. CDD has a strong interest in ensuring that the Commission only approves verifiable parental consent ("VPC") methods that fully comply with FTC's rules and with the underlying purpose of the Children's Online Privacy Protection Act ("COPPA").

Jest8's proposed VPC mechanism should be denied. The proposal fails the requirement that VPC mechanisms be reasonably calculated to ensure the child's parent is the person providing consent and the proposal poses a risk to consumer data. CDD also raises other important information the FTC should address if children are to be effectively protected under the statute.

I. Jest8's Application.

Jest8 proposes a system that uses facial recognition technology to verify identity based on a photograph identification card ("photo ID"). Jest8 refers to this system as "Face Match to Verified Photo Identification" ("FMVPI"). FMVPI involves essentially three steps. First, the

[1] 80 Fed. Reg. 47429 (Aug. 7, 2015).

person uses their smartphone, webcam, or other camera to take a photo of a photo ID. Second, the person takes a photo of themselves. Third, the photos are sent to Jest8, which compares the photos and determines whether the person on the photo ID is the same person as in the second photo.[2] If Jest8 determines the photos match, the consent process is complete. If Jest8 determines the photos do not match, consent would be denied and the person would have to initiate the FMVPI system again.[3] The review process purportedly takes fewer than 270 seconds 95% of the time.[4] Jest8 says it has an agreement with Jumio and its Netverify ID scanning and verification technology to implement the facial recognition-based matching system in the area of children's privacy.[5]

II. The FTC should reject Jest8's proposal.

The FTC should reject Jest8's proposal because it is not reasonably calculated to ensure the person giving consent is the child's parent, and the proposal presents a significant risk to consumer data.

a. Response to question 2: The proposal is not reasonably calculated to ensure the person providing consent is the child's parent.

Jest8's proposal for a VPC mechanism based on facial recognition technology and matching photos to photo IDs fails to meet the standard under 16 CFR §312.5(b)(1) for at least two reasons: first, facial recognition technology is not accurate or reliable enough to be deployed in the sensitive area of children's online privacy; and second, children will easily circumvent the system.

---

[2] Jest8 Application at 2-3.
[3] *Id*. at 3.
[4] *Id*.
[5] *Id*. at 1.

i. Facial recognition technology is not reliable enough to protect children's online privacy.

Facial recognition technology is still not accurate or reliable enough to be used in the sensitive area of children's privacy. The COPPA Rule requires that VPC mechanisms ensure the person providing the consent is the child's parent.[6] Relying exclusively on facial recognition algorithms will undermine that principle because facial recognition has not proven accurate or reliable enough to avoid mismatches or incorrect results and Jest8 has provided no evidence that its proposal is more accurate.

Facial recognition technology has proven inaccurate based on many factors. Facial recognition technology still routinely returns false positives and false negatives based on "environmental factors, the quality of the matching algorithm, the scope of the database, as well as image quality."[7] In the area of law enforcement, the FBI has said "[c]onversion, lighting, angle, [and] resolution" can lead to inaccurate decisions.[8] In a recent review of several commercial facial recognition algorithms, NIST concluded that performance of algorithms varies substantially. In this review, NIST tested six facial recognition algorithms by attempting to match faces to particular photos. For matching faces in high quality photos, the error percentages ranged from 4.1% to 20.5%. For matching faces in lower-quality and webcam photos, which

---

[6] 16 CFR §312.5(b)(1).
[7] EPIC Comments at 7, Face Facts FTC Workshop, https://epic.org/privacy/facerecognition/EPIC-Face-Facts-Comments.pdf.
[8] Samuel Jenkins, Dir. for Priv., FBI, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/sjenkins_dod-facial-recognition-and-privacy_1b.pdf; *see also* Amanda Alvarez, Why Facial Recognition Software Isn't Ready for Prime Time, GigaOm (Apr. 23, 2013), https://gigaom.com/2013/04/23/why-facial-recognition-software-isnt-ready-for-prime-time.

Jest8 will allow in its proposal,[9] the error percentages range from 11.3% to 66.9%.[10] In fact, NIST found that "[a]ll algorithms are intolerant of webcam images, giving elevated miss rates."[11]

Several recent incidents have illustrated that facial recognition algorithms are not ready to be used as a parental verification method. One example involved an algorithm inaccurately identifying a person based on his photo ID. A Massachusetts man had his license revoked because the state's algorithm, which was designed to identify fake IDs, thought his ID was fake. However, his ID was real, he simply looked like another driver.[12] Another example involves Microsoft, which recently released an app that was designed to guess a person's age based on faces in photos. Its algorithms were so inaccurate that they turned into an Internet meme.[13] In the law enforcement context, the FBI uses facial recognition technology for tracking potential criminals that could return inaccurate results up to 20% of the time.[14]

Jest8 does not address any of these issues, nor does it offer any solutions or allege its proposal has better match rates. It allows users to take pictures on their own devices, which will vary widely in quality. Even worse, Jest8 allows use of webcams, which are known for their low quality. Further, Jest8's testimonials and "case studies" do not prove the efficacy or accuracy of

---

[9] App. at 2.
[10] Patrick Grother & Mei Ngan, Face Recognition Vendor Test, Performance of Face Identification Algorithms at 3, NIST (May 26, 2014), http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf.
[11] *Id*. at 24.
[12] Rebecca Boyle, Anti-Fraud Facial Recognition System Revokes the Wrong Person's License, Popular Science (July 18, 2011), http://www.popsci.com/gadgets/article/2011-07/anti-fraud-facial-recognition-system-generates-false-positives-revoking-wrong-persons-license.
[13] Jordan Novet, Microsoft's face-recognition app How Old gets everyone's age wrong, turns into a meme, VentureBeat (Apr. 30, 2015), http://venturebeat.com/2015/04/30/microsofts-face-recognition-app-how-old-turns-into-a-meme-because-it-gets-everyones-age-wrong.
[14] FBI Says 20% Error Rate Okay for Facial Recognition, EPIC (Oct 4, 2013), https://epic.org/2013/10/epic-foia---fbi-says-20-error-.html.

its technology. Without further evidence from Jest8, the FTC should not assume the proposed algorithm will be sufficient under COPPA to protect children.[15]

Jest8 further claims that several large institutions "have used FMVPI to verify identity for a number of years." However, this misleadingly implies that many industries have accepted the technology and have no hesitations about it. Jest8 does not disclose that some industries have been reluctant to implement facial recognition software. In a recent GAO report, the GAO indicated that facial recognition "technology [is] not in broad use by financial institutions because of concerns over its accuracy."[16] Further, Jest8's limited "case studies" show only Netverify's use in situations unrelated to children's privacy (e.g., casinos and Bitcoin retailers) and do not prove the proposal would adequately protect children's privacy.

Thus, facial recognition technology is not robust or reliable enough to ensure children's privacy is protected. However, even if one assumes the technology is accurate enough to protect children's privacy online, this system is easily circumvented.

b. Children will effortlessly circumvent Jest8's system.

Jest8's proposed FMVPI system has another critical flaw: it will be easily circumvented by children. As discussed above, Jest8's proposal requires a person to (1) take a photo of their photo ID, and (2) take a photo of themselves. The singular purpose that this system serves is ensuring that the person *in the photo ID* is the same person *in the second photo*, which leads to an easily circumvented system.

---

[15] While some of the examples used in this section relate to matching a face in a photo to a database full of photos, they still apply to Jest8's proposal. It is quite likely that a person using the FMVPI system will take a photo of themselves that is low quality (which will depend on the quality of the phone camera or the webcam), taken hastily or in dark conditions, or there may be other problems with the photos that could lead to false positives or false negatives.

[16] GAO Report at 12, Facial Recognition Technologies (July 2015), http://www.gao.gov/assets/680/671764.pdf.

Jest8's system would verify the ID holder, but children themselves can get photo IDs that would presumably pass through Jest8's algorithm without problem. Children can get learner's permits and even driver's licenses in many states at age 14.[17] Minors can get a U.S. passport at any age.[18] Given that young children have photo IDs, it could be children themselves that use the system to grant "parental consent." Alternatively, the child could consult an older sibling, an older friend, or essentially anyone with a photo ID to get "parental consent." So long as the person taking the photo is the same person as on the photo ID, the system would appear to be satisfied. This process would be nearly effortless for the child and could occur entirely without the child's real parents ever knowing.[19]

Relatedly, the application does not assert that the proposal would take measures to ensure the person in the photo ID and in the separate photo is the child's *parent*. While this system could likely never establish with 100% accuracy that the person consenting is the child's parent, Jest8's application does not indicate that it checks for certain information that could increase the likelihood of the parent-child relationship. For instance, the proposal does not indicate that its algorithm verifies the birth date on the photo ID to ensure the person is a proper parental age. An ID with a birth year of 2002 or later is extremely unlikely to be the child's parent because that person is thirteen or younger. It is also unlikely that a person under the age of eighteen is a

---

[17] Driver's Licenses in the United States, Wikipedia, https://en.wikipedia.org/wiki/Driver%27s_license_in_the_United_States.

[18] Children Under 16, Dept. of State, http://travel.state.gov/content/passports/english/passports/under-16.html. Minors need a parent's permission to get a passport, but once the child receives the passport, they could use it in any way, including using it with Jest8's consent mechanism.

[19] A child could even circumvent this system by duping a parent into taking a photo of themselves or by taking a photo of the parent for them. In this situation, a child with access to the parent's ID could take a photo of the ID, then ask to take a photo of the parent without providing further information, and the "consent" would be "verified" again without the parent knowing what happened.

parent, which means Jest8 could probably filter for any birth dates past 1997. Though, if Jest8's algorithm did verify birth date, it must delete that information promptly after collection to minimize risk to consumer data.[20]

Jest8's proposal authenticates the identity of the ID holder, not the parent-child relationship. The FTC made clear when it rejected AgeCheq's second VPC application that mechanisms that authenticate something other than the parent-child relationship would be rejected. In AgeCheq's case, the proposed system "authenticate[d] the device rather than the user."[21] In Jest8's case, the proposal authenticates the ID only, not the parent. Thus, the FTC should reject this application.

III. Response to question 3: The method poses a risk to consumer data.

There are several reasons that this method poses a risk to consumer data. First, the proposed process is used for data extraction in other contexts. Second, the "Netverify" privacy policy indicates Jumio, the company that uses this system in other contexts, collects extensive data about users. And third, Jest8 has little to no track record in privacy protection, including addressing the interests of children.

The same photo ID authentication system is used in other contexts to extract data from photo IDs. For instance, the video provided by Jest8 in its application (https://vimeo.com/118353806) explicitly states that the Netverify software "accurately capture[s] the image for authentication *and data extraction*."[22] Other similar systems are used for

---

[20] 78 Fed. Reg. 3972, 3987 (Jan. 17, 2013) ("operators [must] delete such data immediately upon verification.").
[21] Letter, Donald Clark, Sec. of FTC, to Roy Smith II, CEO AgeCheq, https://www.ftc.gov/system/files/documents/public_statements/621461/150129agecheqltr.pdf.
[22] Jumio Netverify, Vimeo (Jan. 31, 2015), https://vimeo.com/118353806 (0:41-0:48) (emphasis added).

data extraction as well, including "Document Verification and Face Match" from Identity Verification Services, which will "capture the face of the user while verifying and extracting the data from driver [sic] license, identity card and passport."[23] Jest8's proposal is adapted from contexts where one of the primary purposes of the system is the collect and extract data about people. Thus, the FTC should be wary of claims that applicant will delete the collected data. One potential solution, as discussed in the COPPA Statement of Basis and Purpose, would be to limit collection of "identification information to only those segments of information needed to verify the data."[24] If the system verifies photos, it could blur other data and only verify photos.

The Netverify privacy policy describes practices that would be alarming in a COPPA context. The privacy policy discloses that Jumio may collect, through Netverify, "name, physical address, email address, telephone number, social security number, driver's license number, state or national ID card number, passport number, other ID card number, credit or debit card number, CVV, expiration date, and/or date of birth."[25] Jumio may also collect "a visually scanned or photographed image of your face and/or your identification card, driver's license, passport, utility bill, bank account statement, insurance card, or credit/debit card."[26] Jumio shares all data it collects with "Third Party Data Controllers," which include its clients and other third parties with which Jumio does business.[27] Jest8 has not provided any proof or verifiable plan, only mere promises, that it will delete its data. It further provides no proof or plan that it will not share the

---

[23] Document Verification and Face Match, Identity Verification Services, https://identityverification.com/product/identity-and-biometric-face-match/?doing_wp_cron=1442087761.5666038990020751953125.
[24] 78 Fed. Reg. 3972, 3987 (Jan. 17, 2013).
[25] Netverify Privacy Policy, Jumio, https://www.jumio.com/legal-information/privacy-policy/jumio-inc-privacy-policy-for-online-services.
[26] *Id.*
[27] Netverify FAQs, Jumio, https://www.jumio.com/faqs/netverify-en (indicating the company shares the data with the requesting company).

extensive amount of data it will collect through this system with third parties. These practices are unacceptable under COPPA and should preclude approval of this application.

Last, applicants appear to have little experience with protecting anyone's privacy, much less children's privacy. Jest8 and Riyo are relatively new companies. They were incorporated in December 2013 and have few assets.[28] Tom Strange, Director of Jest8, has a background as a chartered accountant.[29] Mr. Strange's lack of qualifications calls into question his ability to properly protect children's privacy through his software. CDD is concerned that the system proposed in the application would put children at risk unless the FTC engages in a detailed analysis of the proposal, the companies involved, and their background.

IV. Conclusion

There are several reasons to be concerned about the Jest8 proposal. It is not reasonably calculated to ensure the person providing consent is the parent. Facial recognition technology is not yet where it should be to be deployed in the complex and important context of children's privacy. Further, the proposal is easily circumvented by children and is designed only to ensure the person in the photo ID is the person in the second photo. It does not ensure the person consenting is the parent, or even a relative, of the child. Last, the risks to consumer data are too high to approve this method. This method is used for data extraction in other contexts, which is

[28] Information about Jest8 Limited, UK Data Centre, http://ukdatacentre.co.uk/company/08797832/JEST8+LIMITED; Information about Riyo Verified Limited, DataLog, http://www.datalog.co.uk/browse/detail.php/CompanyNumber/08797832/CompanyName/JEST8+LIMITED; Information about Riyo Verified Limited, DueDil, https://www.duedil.com/company/08797832/riyo-verified-limited/financials.

[29] Information about Thomas James Edward Strange, UK Data Centre, http://ukdatacentre.co.uk/person/1789206/Mr+Thomas+James+Edward+Strange

confirmed by the Jumio privacy policy. Also, the applicant lacks experience in this area and at the very least that should raise doubts as to applicant's ability to truly protect children.

Respectfully submitted,

/s/Eric G. Null

Eric G. Null
1375 Kenyon St NW
Apt. 515
Washington, DC 20010
Eric.g.null@gmail.com
Counsel for Center for Digital Democracy