WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum to the Federal Trade Commission regarding
Proposed Consent Order, *In the Matter of Everalbum, Inc., File No. 192 3172*

Via regulations.gov

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex D)
Washington DC, 20580

23 February, 2021

Dear Commissioners:

Thank you for the opportunity to comment on the proposed consent order in the matter of Everalbum, Inc. In its complaint, the Commission alleges that Everalbum misrepresented to its users the circumstances in which the company would utilize face recognition on its users' photos. The Commission's complaint also alleges that Everalbum utilized improperly acquired face templates (biometric analysis) of some of its customers to enrich its commercial biometric algorithms (*In the Matter of Everalbum, Inc*., Complaint, 11-12. https://www.ftc.gov/system/files/documents/cases/everalbum_complaint.pdf), an activity that the FTC alleges went beyond the scope of what Everalbum told its customers. (Complaint, 16).

WPF has long worked in the area of biometrics, having both researched and published extensively in the area. See Pam Dixon, *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S., S*pringer Nature, Health Technology. DOI 10.1007/s12553-017-0202-6. http://rdcu.be/tsWv. Open Access via Harvard- Based Technology Science: https://techscience.org/a/2017082901/. See also Pam Dixon and Bob Gellman, *Without Consent*, World Privacy Forum, April 2020 pages 71-97 regarding face recognition and children. (https://www.worldprivacyforum.org/wp-content/uploads/2020/04/ferpa/without_consent_2020.pdf)

Biometrics are math, not magic, and each type of biometric has a set of vulnerabilities. Face recognition systems have now been proven to have significant risks and challenges by multiple studies, but in particular it is the rigorous 2-year NIST Face Vendor Recognition Test study on demographic impacts of face recognition that provides the most accurate and complete documentation on the age, gender, and racial bias in face recognition systems. (See: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf).There is no longer a question mark regarding the problems in face recognition technology; age, gender, and racial bias are salient characteristics in these systems at this time, in differing levels depending on the system, algorithm, and utilization. The result of these now-well researched findings is that we know that face recognition systems carry more risk than, for example, a simple photo album app that just stores photos.

In these comments, we address several aspects of the proposed consent order. We discuss policy issues, and we also, where necessary, discuss some of the technical language. The field of biometrics utilizes many terms of art that reflect the precision, actions, and structures of the technology. These terms can be unwieldy, but they are nevertheless quite important for accuracy in communicating about face recognition systems.

I. Recommended Changes to Definition B, "Biometric Information"

The definition of biometric information in the proposed order introduces some technical inaccuracies. It is important to ensure that any image from which one can extract an identifying template becomes subject to protection under the order. We propose the following definition, which is accurate on a technical level, and is as inclusive as the proposed definition.

> Biometric data means an individual's physiological, biological or behavioral characteristics that can be used, singly or in combination with each other or with other identifying data to establish individual identity. These include but are not limited to imagery of iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template (e.g. a faceprint or a minutaie template or voiceprint, etc.) can be extracted as well as keystroke patterns or rhythms, gait patterns or rhythms, sleep health or exercise data that contain identifying information.

This is a definition crafted by leading biometricians with WPF. See also the NIST reference on the Face Image Standard, https://www.nist.gov/system/files/documents/2016/12/12/griffin-face-std-m1.pdf as well as ISO-19794-5 FDIS, Final Draft International Standard of Biometric Data Interchange Formats, Part 5, Face Image Data. https://www.iso.org/standard/50867.html. We encourage the Commission to use existing terminology of the biometrics field, as it is extremely precise, well-defined and understood now for many years.

II. Support for Definition C, "Clearly and Conspicuously"

We support the definition of "clearly and conspicuously" in C (1-8).

For C (6), we recommend that the wording be broader, and more clearly inclusive of videoconferencing types of interactions.

The current language states:

> The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

This language could be improved by noting that the disclosure must:

> .....comply with these requirements in each medium through which it is **sent or** received, including all electronic devices and **communication types, including** face-to-face, **online video and videoconferencing media, and others.**
> [bolded terms are the additions.]

The term "face to face communications" may possibly be construed to mean only in-person communications and not to include videoconferencing and/or visual messaging apps.

III. Recommended Changes to Definition of "Face Embedding" in E

In E, face embedding is said to mean "data, such as a numeric vector, derived in whole or in part from an image of an individual's face."

Face embedding is a complex and technical topic. For the purposes of the consent order, it is important to recognize two distinct types of face embedding: deterministic, and probabilistic (PFE). The consent order's existing definition likely only covers deterministic embedding. Unless the order clearly covers probabilistic face embedding (PFE), the order may potentially not cover all current or future behavior of the company.

To correct the definition, we recommend the following language:

> Data, such as a numeric vector, derived in whole or in part from an image of an individual's face **that give a point estimation, and/or data such as probabilistic face embeddings (PFEs) which give a distributional estimation.** [bolded terms are the additions.]

The most important resource on this topic is *Probabilistic Face Embeddings*, Yichun Shi and Anil K. Jain, Michigan State University, 2019. Available at: https://arxiv.org/pdf/

1904.09658.pdf. Other authoritative documentation includes the NIST reference on the Face Image Standard, https://www.nist.gov/system/files/documents/2016/12/12/griffin-face-std-m1.pdf, as well as ISO-19794-5 FDIS, Final Draft International Standard of Biometric Data Interchange Formats, Part 5, Face Image Data. https://www.iso.org/standard/50867.html.

IV. Support for Notice and Affirmative Consent Provision; Recommend Adjustment to Some Language

WPF supports the affirmative express consent provision in Section II, A-B. We encourage an edit to the language in the first paragraph in order to correct a potential technical loophole.

The current language in the opening graph of Section II reads:

> ....prior to using Biometric Information collected from a User to (1) create a Face Embedding "or (2) train, develop, or alter any face recognition model or algorithm, must .....

We recommend the language be updated to be more technically accurate, to read:

> ...prior to using Biometric Information collected from a User to (1) create **any type of** Face Embedding or (2) train, develop, **utilize, update**, or alter any face recognition model, algorithm, **or system** must ..... [bolded terms are the additions.]

We encourage the Commission to recognize that with face recognition technologies, there are typically many components inclusive of algorithms and models, but that go far beyond just that. The proposed order is not comprehensive as it is currently written.

V. Support for Deletion Requirements

WPF supports the deletion requirements set out in Section III, Deletion, A-C.

Specifically, WPF supports the requirements set forth in A.

In B, we recommend broadening some of the language to create more technical accuracy.

The proposal uses the following language to describe deletion requirements for face embeddings: "...delete or destroy all Face Embeddings derived from Biometric Information Respondent collected from Users ....."

We suggest the following additions to the existing language:

> "...delete or destroy all **biometric** face embeddings, **deterministic and/or probabilistic, based upon and/or derived from any images or other information collected from users.** [bolded terms are the additions.]

The reason "or other information" is important is because some embeddings utilize more than just the deterministic or probabilistic data points to include things such as a name, age, etc.

VI. Request for Public Dissemination of Compliance Reports.

We support the compliance monitoring provisions in the proposed order. We request that the compliance reports are made public by the Commission proactively, rather than requiring members of the public to rely on Freedom of Information Act requests after the fact.

Face recognition systems carry significant risks to individuals, including risks relating to discrimination and bias against vulnerable populations. It is in the public interest for compliance documents to be made public proactively. We understand that there may be a need to redact some information, and we are not requesting that such information be inappropriately unmasked. We merely ask that the compliance reports be made public affirmatively by the Commission as part of the order due to the significant public interest.

VII. Monetary penalty

The Commission made a compelling case that the behavior of Everalbum violated the FTC Act § 5. However, the Commission did not provide a monetary penalty. The lack of a monetary penalty for violative behavior is unacceptable in today's world which increasingly focuses on compliance.

In discussions about federal privacy legislation, many point to the Commission as a key player in data protection compliance. No-money consent agreements in cases where there are clear violations could undermine the Commission's reputation at a sensitive time.

VIII. Conclusion

Thank you for your work on this case and consent order. It is a precedential consent order, and we encourage the Commission to:

1. Amend language to be more technically accurate,
2. Retain the provisions regarding required deletion of images as well as algorithms and face embeddings, and
3. Publicly disseminate future compliance reports.

If there are any questions we can answer or assistance we can provide, we stand ready to help.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum