PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

22nd October 2019

Dear member of Yoti's Guardian Council,

We are writing to you in your role as a member of Yoti's Guardian Council. In a recent consultation response to the UK government, we called upon the UK to develop "a digital identity ecosystem that becomes a world-leader in respecting the rights of individuals and communities"[1]. Unfortunately, Privacy International is concerned that Yoti is not meeting this promise, through the way that Yoti user data has been treated for their Yoti Age Scan product.

As we highlighted in our recent post on the subject[2], this is a development that has raised serious concerns for Privacy International about Yoti's use of users' data. As you are aware, Yoti process personal data, being gender and year of birth taken from a government issued or other official national identity document, together with a photograph of an individual. The processing is carried out as part of a training dataset to train Yoti's Age Scan technology, which is used to estimate an individual's age.

The privacy policy Yoti had in place up until August 2019 and app itself were wholly inadequate in explaining how customer data was used to develop Yoti's Age Scan technology. For your interest, we set this out in Annex A. This privacy policy has been replaced at least twice since we met with Yoti.

We further noted to Yoti that their privacy policy stated they were tagging an individual's ethnicity. Ethnicity is special category data according to the General Data Protection Regulations. In responding to us, Yoti stated that this was an error and instead it should refer to tagging skin tone.

In Privacy International's opinion, in adding Yoti users' data to a training dataset used to train age verification technology, Yoti were using their customers' data in a way they would not reasonably expect and for a purpose other than which they provided it, raising questions as to the fairness of this use and the principle of purpose limitation, both of which are core tenants of data protection.

The most recent privacy policies (August and September 2019) have seen some improvements, which are to be partially welcomed.

Privacy International understands that Yoti stores the data used for Yoti Age Scan (details from the passport of the user, plus their photograph) on a

[1] https://privacyinternational.org/advocacy/3215/response-uks-call-evidence-digital-identity
[2] https://www.privacyinternational.org/long-read/3254/identity-gatekeepers-and-future-digital-identity

separate R&D server, and that they cannot access information like name to identify the user. However, this does not change the fact that – for many users – the use of their data to train the Age Verification algorithm would remain unexpected, and the lack of an 'opt-in' system makes it challenging for the new user to *not* have their data as part of this dataset.

In our engagement with Yoti, we have also asked Yoti for the publication of parts of their legitimate interests' assessment of Yoti Age Scan. We do this in order to better understand the basis for processing what they declare in their privacy policy to be biometric data. While not requiring the publication of the full assessment, our request mirrors the Article 29 Working Party Guidance, endorsed by EDPB, on data protection impact assessments which states:

> *"...controllers should consider publishing at least parts, such as a summary or conclusion of their DPIA. The purpose of such a process would be to foster trust in the controller's processing operations and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation."*

Further, the Article 29 Working Party Guidelines on Transparency, endorsed by the EDPB, state in relation to 'legitimate interest':

> *"As a matter of best practice, the controller can also provide the data subject with the information from the balancing test, which must be carried out to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data...In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly..."*

We would like you to join us in asking Yoti:

- To actively communicate to customers whose data formed part of the training dataset. We want to ensure that users are aware of how their data has been used. Yoti have informed us they have no way to contact their users to do this. However, even so, Yoti could take steps to reach out to their users: through a notice on the app, public communication, and notices at the places where people use Yoti.
- To develop an 'opt-in' approach for the use of user data in such R&D initiatives like Yoti Age Scan, rather than an 'opt-out' hidden many menus deep on a setting screen.
- To publish the relevant sections of their legitimate interests' assessment of Yoti Age Scan.

We would also ask the Guardian Council to reflect upon the processes within Yoti that led to the initial launch of a product like Yoti Age Scan with such an inadequate privacy policy or explanation for users, and without any opt-out in place. Similarly, we would ask that the Guardian Council explore whether

the case of Yoti Age Scan reveals a concern about the architecture of Yoti. Yoti has been keen to emphasise with us in our communications that: "Yoti has deliberately architected its platform to not have access to a consumer's data, after the initial anti-fraud review." However, the case of Yoti Age Scan draws attention to the apparent situation where Yoti does have continued access to data provided by users: on its R&D server, where it is added at the point of the user uploading a document. There is nothing *architecturally* to prevent additional data fields to be included from future uploads of identity documents by existing or new users; nor is there anything *architecturally* to prevent that data to be used for the development of other products (for example, other algorithms) in the future.

Furthermore, we would call upon the Guardian Council to consider carefully any future developments at Yoti that involve the use of user data for new purposes. If we see a situation where digital identity companies are earning their keep from the use of data outside of the core provision of identity, then we risk both the public trust and a distortion of the market. These distortions will lead to activities not to the benefit of the user, but one in which the user is a mere product.

If you have any questions, please do not hesitate to get in touch.

Yours sincerely,

Privacy International

Annex A: Yoti's privacy policy

For a number of years, Yoti's privacy policy failed to provide transparent, clear and accessible information to data subjects whose photograph, year of birth and gender were processed for the purposes of Age Scan, and whose faces are tagged with ethnicity / skin tone information. It is necessary to read the entire privacy policy to understand the lack of transparency.

The version we review below was in place until July 2019[3]. Yoti states in its 2019 White Paper[4] that it used 35,301 facial images of verified age, taken from Yoti users for the 23 April 2019 testing of the Yoti Age Scan model. It is unclear from what date they started collecting user data for the purposes of developing Age Scan.

On page 5 the privacy policy 'Information collection and use' it stated:

"We collect information to set up your Yoti account, when you add documents and when you use the app."

"We use it to do things like … check the documents you add are genuine and the photo matches your account set-up photo; verify details; ***check for fraud****; authenticate you when you make certain requests such as to delete your account."*

This reference to fraud implies checking for fraud in relation to a user's own Yoti account.

On page 6, in relation to 'Your photo' there is no statement at this point in the privacy policy that this photo might be used in Age Scan. However, this is the photograph that is added to the training dataset.

In relation to the photo the privacy policy states:

"Your photo: To have a photo on your account that you can then share. After registering you are able to take an account photo, which you can then share as part of proving your identity. We also ask you to take a photo when you take certain actions in the app, so we can be sure it's you. Organisations may also request this as an extra security step. … Yoti securely stores the photos. We keep this information until you or we close the account and delete the information."

On page 12, in relation to 'Information from Government-issued or other official identity documents' the privacy policy states:

"While we verify your identity, the information is kept securely but our Security Centre can access it, and may do so for training, compliance and quality assurance purposes. We can only access this information up to seven days after verification."

Again there is no mention of Age Scan in this section despite the fact that date of birth and gender are taken from this document and used, together with the photograph, to train Yoti's Age Scan technology.

Details regarding Age Scan were only added to the Privacy Policy in January 2019 version. They are in a completely separate section to the sections which are specific to the data types.

In relation to Age Scan the privacy policy states on page 14:

[3] yoti.com/wp-content/uploads/2019/07/Yoti-privacy-information-Yoti-app-22-July-2019.pdf
[4] https://s3-eu-west-1.amazonaws.com/prod.marketing.asset.imgs/yoti-website/Yoti-Age-Scan_Digital.pdf

"You can use our age estimation technology, Yoti Age Scan, to estimate your age. That way, you can prove your age without adding an ID document to your Yoti account. Yoti Age Scan instantly estimates whether you're above a certain age threshold, such as 18+. It doesn't estimate your actual age. It works by using the digital map of your face we captured when you created Yoti. When you choose to use this feature in the app we send a copy of the digital map of your face from your Yoti to our servers. After the age estimation we permanently delete it. Your original digital map is stored securely."

"You can remove you estimated age from your Yoti at any time by replacing it with your date of birth from an ID document."

"When you look older than a certain age threshold, Yoti Age Scan can confidently estimate that you're above that age once it takes estimation errors into account. If you get an error message it might be that you look too young for Yoti Age Scan to confidently estimate that you're over 18, which is our minimum estimated age threshold."

It is not until a section entitled 'Biometrics' that internal research and development is mentioned, on page 36. Confusingly, given that Yoti process data based on legitimate interests, their definition of biometrics is not the same as understood by data protection legislation.

"Internal research and development

As well as preventing fraud in your everyday use of the app, we need to make sure our checks continue to work and that we constantly improve … We have an internal research and development team who are constantly testing new ways to prevent fraud and to do their job, or sections of the video or phone movement measurements. To test and improve our age verification technology they use photos, year of birth and gender. We also manually tag some data with information on ethnicity or skin tone.

…

The research and development team don't have any other information, and non that could identify you personally."

The use of fraud here seems undeniably linked to the App, not wider research such as Age Scan.