Dear [redacted]

Thank you for your email and the opportunity to respond to the article. We disagree with pretty much every section of your blog and again, would welcome the opportunity to explain to your team how Yoti works, the ethical framework it is founded on and our business model.

In October 2017 Privacy International took part in the workshop run jointly with Consumers International on peer-to-peer transactions. We have invited Privacy International to participate in the APPG Digital Identity, which kicked off in December 2017. In January 2019, we invited the Privacy International team to take part in civil society review of Yoti's age estimation approach at the early stages of its design; however you chose not to participate.

Given the meeting we had with you in July and the clarifications we provided, we are surprised by the tone of this piece, the frequent use of negatives and the short requested turnaround time to give you a considered response. As we outlined when we met there have been in-depth reviews of Yoti undertaken by independent bodies such as CDT and Dr Allison Gardner, IEEE accuracy of algorithm & bias expert.

Yoti's approach is designed specifically to put the user in control; they can see clearly what they are being asked to share, have a receipt of the data they share. The app is designed with data minimisation in mind, that just certain attributes can be shared, rather than all the data from an identity document.

Your conclusion seems to be that no use of data is legitimate unless the individual in question gets a direct personal benefit. To follow this to its conclusion, if everyone followed this approach, there would be no medical research, no research on preventing poverty, stopping crime or addressing public health issues.

You also seem to view digital identity as an inherently negative technology development; rather than considering how it can also have positive societal benefits, in terms of for instance safeguarding or fraud reduction.

We reiterate that the core purposes of the app biometrics and our R&D work are fraud prevention, safety and security.

We have provided comments inline in blue. We similarly reserve the right to publish our entire response to you.

Kind Regards,

[redacted]

***The Identity Gatekeepers: Looking towards the future of digital identity***

***Digital identity providers***

*Around the world, we are seeing the growth of digital IDs, and companies looking to offer ways for people to prove their identity online and off. The UK is no exception; indeed, the trade body for the UK tech industry is calling for the development of a*

> *"digital identity ecosystem", with private companies providing a key role. Having a role for private companies in this sector is not necessarily a problem: after all, government control over ID is open to abuse and exploitation. But we need to ask what we want this industry to look like, and how we can build one without exploitation. These are the new digital gatekeepers to our lives.*

Yoti comment: We think it is healthy that there is civil society participation to look at how digital identity can be seen as a tool for individual empowerment, providing universal access to services, rebalancing the current digital and data paradigm in favour of the consumer or citizen.

We would disagree with the claim that all private companies offering digital identity are the 'new digital gatekeepers to our lives', Yoti in particular lets the individual act as gatekeeper to their own data, we do not decide when or if an individual uses their Yoti, for instance to better manage their passwords, to share information peer to peer, with a company or with a Government.

We publish transparently our business model and pricing.

> *In our response to a recent UK government consultation on digital identity, we highlighted the imperative of avoiding a future for digital identity that exploits the data of individuals. This is an imperative, given how these companies are becoming gatekeepers to access key services, both online and off. People increasingly either have to use their services to go about their lives, or life becomes difficult without them. Thus, they are in a powerful position. At the same time, proving your identity is something that most people don't really want to spend a lot of time thinking about. This is a powerful combination that leaves opportunities for abuse.*
>
> *As we look towards what the future will look like for digital ID, we must not see one in which companies in the digital ID industry are able to exploit our trust and take advantage of their position in the market. The burgeoning digital ID industry deserves our attention, and potential abuses must be brought to light.*
>
> *The norms surrounding this nascent industry must be explored; it is essential that the questions as to how this industry should behave are key. So, what kind of issues need addressing in this industry? One of the key ones, that we shall discuss, is that of businesses using your data for other purposes.*

Yoti comment: we agree and this is why we have designed a clear ethical framework with clear principles and set up an external ethics council with experts from the human rights, consumer rights, last mile tech, and online abuse fields, to hold Yoti to account. The terms of reference and minutes are published openly. We are also a BCorps, meaning we are committed to growing profits and purpose; and making decisions not just based on shareholder value, but also considering good governance, the community, staff, the environment, the supply chain.

In today's world a young person at a nightclub or a retailer can be obliged to share all of the details on their driving licence, including their home address, with staff. Yoti in contrast enables the anonymous sharing of just an over-18 attribute.

Yoti is also working with NSPCC childline, to enable under 18s who wish to request the removal of sexting pictures without having to to share their passport or driving licence details to prove they are under 18. Using Yoti, 13-17 year olds can anonymously share their under-18 attribute. Another example of data minimisation.

At some point time in 2020, it is envisaged that approx 20m British citizens will need to prove they are over 18 to access adult content. Yoti's Age Scan (age estimation AI) will allow anyone looking over 21 to not enter any personal details into any adult site or AV provider but instead be age estimated. To recap, Yoti does not store the image, it is instantly deleted. Those aged 18 to ~21 can use the Yoti app to anonymously transfer their over-18 attribute with an adult content site to protect their privacy.

> *Using your data for other things: the example of Yoti*
>
> *An example of this is the UK-based digital identity provider, Yoti. Since the introduction of the Yoti app in 2017 it has been downloaded over 3 million times.*

Yoti correction: The current download figure is over 5 million.

> *Operating through its app, Yoti makes use of government-issued ID documents (for example, passports) to verify the identity of its users.*

Yoti comment: we feel this sentence is misleading. If a user chooses to use Yoti and chooses to add an ID document, we carry out security checks on the document to make sure it is valid, and that they only upload their own document. We provide the verified identity for a user. The user then has verified identity details they can share when they need to prove their identity or age. A user can also choose to share details peer to peer.

Without Yoti, internet users would sometimes have to email or upload or scan their ID documents to websites requiring ID verification. Yoti provides Yoti users with a choice to minimise the verified details they need to send to a website for ID verification.

Consumers International worked with Yoti to look at how digital identity can build trust in peer-to-peer transactions, as highlighted in their blog and workshop, attended by [redacted] of Privacy International.

*Participants also found out more about new innovations in Digital ID provision, which could be a game-changer in terms of how we verify our identity online. We are seeing new tools that link up physical proof you are who you say you are with official documents, thus creating a verified, portable Digital ID. With this ID you can log onto websites without having to re-enter information each time. It makes things easier, more legitimate and helps you control the amount of information you are giving people. For example, if a website only needs to know your age, your digital ID can simply confirm that you are over 18, as opposed to having to provide your full date of birth. (Consumers International Blog)*

> *Users are also required to take a 'selfie' of themselves for the purpose of having a photo on the account.*

Yoti comment: The phrase above is incorrect. Users are not required to take a profile picture at onboarding. This is an option for them after onboarding. If they add a profile picture it is available for them to share along with other details they add.
To keep all users safe, Yoti requires a liveness test to ensure real people are creating a Yoti and the biometric template retained from the liveness test is used to ensure only the Yoti account owner can use their live face to re-authenticate themselves within their account. All this is clearly explained up front in our biometric consent copy.

> *This photo can be "shared as part of proving your identity." Yoti states the purpose of their biometric identity app is to "provide you with a quick, easy, secure and privacy-friendly way to prove your age and / or identity, online and in person". If an organisation accepts Yoti, then you can share details that have been verified by Yoti and taken from the ID documents you have uploaded to the Yoti app. The app includes welcome features, like the ability to only share particular attributes – for example, the ability to only share the fact that the user is 'over 18', rather than sharing all the information on their ID.*
>
> *Yoti is used not only by private businesses, but also the government of the States of Jersey; the Improvement Service (for local government) in Scotland; and is a pre-ticked option when applying for a CitizenCard proof of age card. Yoti also works globally, with an office in India and research into ID in Africa.*

Yoti comment:
NB States of Jersey is the correct wording.
Please can you clarify that the CitizenCard you are referencing is the Yoti-branded one, not the standard one? If someone wants to set up a non-Yoti CitizenCard then nothing is pre-ticked. It is important to note that CitizenCards are data minimised, so a young person is able to share less information than on a driving licence or passport to prove their age, and also more price accessible to young people on lower incomes.

We feel the reference to Africa as it stands is misleading. We have no Yoti app operations in Africa. Our social impact research and work has included discussion with local groups in 10 African countries and 7 Asian countries. We have recently funded three fellowships as part of research into ID and one of these in in Africa (the others are in India and Argentina). These are not about Yoti products or services, they are research into specific identity issues in those countries.

Yoti has publicly committed to offering its Yoti Keys technology on an open source basis and free to charities, as part of the global efforts to help reduce the 1.1 billion people without formal identity, as highlighted in the UN Sustainable Development Goal 16:9.
More info here: https://www.yoti.com/yoti-digital-identity-fellows/

> *The concept behind the core Yoti offering is not unproblematic. Big Brother Watch has criticised Yoti's part in a growing "casual use of biometric checks".*

Yoti comment: we strongly refute this statement. We are very surprised by your double negative comment and tone here. The concept behind the core Yoti offering is to provide a consumer-centric, privacy-friendly and secure way to prove ID / age, with a focus on only sharing the information necessary for the situation in question (as you reference above with regard to proving over 18 rather than sharing a date of birth).

The biometrics aspect provides an extra layer of security and assurance which allows individuals to be sure that the other person is who they say they are. It also provides assurance that the ID document the verified details came from actually belongs to the user in question. It is a long way from the surveillance and government misuse of data concerns that BBW and others have, and that are referenced at the end of the article you cite.

Given the current alternatives where individuals have to hand over entire ID documents to be scanned or photocopied, we are surprised PI does not proactively support a more privacy-friendly approach to proving age in age-restricted environments. Currently 1.4[1] million[2] people lose ID documents in the UK each year and are as a result at increased risk of identity fraud. This begs the question, would the author of the blog and BBW prefer that 1.4 million UK citizens 'casually' lose their documents annually and end up at higher risk of identity fraud?

Yoti also provides users with the option of a free integrated password manager, to help people to avoid having weak passwords.

Leaving a biometric trail is a deterrent for fraudsters. The use of multi-modal biometrics is also recognised as key in the war against fraudsters. Regulation such as the 5th anti-money laundering regulations and Payment System Directive 2 (ALM5 and PSD2) are requiring digital forms of identity verification, as face-to-face physical document checking without trained document specialists and access to sophisticated equipment is insufficient to deter fraudsters. Fake ID documents are now available very inexpensively online and only the most highly trained operatives are able to review international documents from over 180 countries around the world.

Research from 2017 (details below) states that staff in customer-facing environments face verbal, physical and racial abuse when checking ID and age, and in many cases do not have the training to determine if a document is valid or not, or if it belongs to the person holding it or not. Retailers and retail staff affected may take a different view of biometric checks, as something that can deter staff from being the subject of abuse.

https://www.underagesales.co.uk/user/Abuse%20and%20Violence%20Report%202.pdf
*2017 research undertaken by One Poll for Under Age Sales suggests that there are almost 6,000 incidents every day of store workers experiencing verbal or physical abuse as a direct result of asking customers for ID to purchase age restricted products. A third of retail workers say that abuse has left them less confident in asking for ID. Shop workers from ethnic minorities were found to suffer the most, with 33% of Asian or Asian British workers saying they are typically verbally threatened or abused on a weekly basis. More than a third of workers (38.43%) indicated that they were verbally abused at least once a month, with one in 7 (14.05%) reporting being abused verbally either weekly or more often. That would suggest that around 55,000 shop workers are verbally abused at least every week, just for asking for ID. Around one in 14 shop workers report being physically attacked at least once per month (7.11%). Taking a 'best case scenario' with those being assaulted in at least one incident per week and so on through the responses, this would indicate that an average of 1.74 assaults against each shop worker every year. With 390,000 shop workers in the UK, that would indicate some 678,600 assaults per year, or 1,860 every day.*

[1] https://www.gov.uk/government/news/report-your-lost-or-stolen-passport
[2] https://www.gov.uk/government/news/drivers-lose-almost-a-million-licences-in-the-last-year

> *Privacy International has critiqued the extent to which identification systems can truly capture a complex, changing, essential thing like 'identity', resulting in discrimination; concerns echoed by researcher Zara Rahman.*

Yoti comment: Yoti is clear that our app is about proving the identity / age as contained in official ID documents issued to a person. Therefore this sentence is misleading in the context of this piece being about the Yoti app.

We agree that identity is complex and changing. For example, we are engaging with Sparkle, a leading transgender charity, to understand how Yoti can support communities whose identities are in transition or have changed over time.

Yoti has been asked to support the ESPRC funded Centre for Digital Citizens (CDC) at Northumbria University & Newcastle University ESPRC project looking at the 'safer digital citizen'.

> *Privacy International's research has shown that identification requirements are a major source of exclusion for those who lack access to identification:*

Yoti comment: We agree and this is why we have developed other mechanisms for individuals without identification to prove ID / age. Yoti Age Scan is one such solution. Approx 24% of young adults and older adults do not own either a passport or a driving license and suffer varying degrees of social exclusion. Our social purpose work, Fellowship Programme and our Yoti Keys development also aim to investigate solutions to prove identity or age, including in instances when people have no official ID document.

Yoti via the Yoti Foundation has also supported the research of The Engine Room, alongside the Omidyar Foundation and the Open Society Foundations - undertaking research and analysis on both the effects of digital identification technologies and the experience of those advocating for better outcomes. A partnership with local researchers in the Global Voices AdVox network grounded the research in lived experience across diverse contexts. Through local focus groups and cross-border analysis and collaboration, the research team identified and seeded networks of allies for future advocacy and collaboration, and began a dialogue on ways to raise the effectiveness of CSO contributions to Good ID.

In the UK, Yoti has also proactively worked with CitizenCard which provides lower-cost proof-of-age documents, mainly to young people who do not have another ID document for travel or driving.

> *But we must also ask what Yoti is doing with the data of the users of its app: Yoti is in a privileged position of having access to the data on an individual's official ID, like a passport: a 'gold-standard' for identification that few apps or services would have access to.*
> *Similarly, they have access to the image of a person's face ('the selfie'), verified to be theirs against that same document. What do they do with this information, besides their core offering of identity and attribute verification?*

Yoti comment: This paragraph needs to be removed as it is factually inaccurate. The entire point of Yoti, as you know, is that we have not built a relational user database in the way

many other companies have. Yoti is deliberately architected as a non-relational database so that once your account is set up, only you can access your own data. We cannot. We think your statement is misleading as it suggests an access that does not exist. A failure to explain this important security aspect properly fails your audience.

If your concerns are the use of user data for R&D, we think it is important to distinguish between a general notion of access and what actually happens in practice at Yoti - that limited user data for this work is sent to a secure, separate R&D server at specific points. This is very different to the notion of a user database of identity data that a company can access at any time.

> ***Yoti Age Scan***
> *In April 2019, Yoti launched a new initiative, and potential income stream for the company: Yoti Age Scan technology. This product - described by Yoti as "using Artificial Intelligence (AI) for good" - estimates an individual's age based on their image. This is used, for example, within the Yoti app for those who have not uploaded a verified ID document that contains their age; at self-service checkouts to see if an individual is old enough to buy alcohol; to access social media services aimed at teenagers; or to access adult content online. Yoti charges businesses 15 pence (£) a pop to identify the age of a face.*

Yoti comment: the pricing information for Yoti age estimation is incorrect. The 15p cost is for a once only required **age verification** of a customer account based on a verified date of birth that has come from an ID document. The enterprise cost for using Age Scan API to **estimate age is £0.01** per check based on volume of checks. There are high-volume discounts available on asking and tiered pricing for volumes less than 10m, as detailed transparently on our webpage. There are no integration fees.

The second concern we have with the final sentence in the above paragraph is the use of the verb 'identify' in relation to a technology that does not in fact identify you. This is misleading as Age Scan **estimates** the age of a face; the image is not stored to disk, it is instantly deleted.

Yoti provides the core platform free for eligible non-profits; and advanced services at reduced rates for non profits, such as digital signatures. Yoti Age Check solution is provided free to convenience stores (taken up by over 9000 so far) and our Yoti app AV solutions are free to the BBFC regulated adult-content providers, as per our commitment made 3 years ago, to ensure adult content sites did not have problems, on cost grounds, to adhere to regulation to reduce access to adult content by minors.

According to the Electoral Commission, over 24% of the UK [3]population does not have a photo ID document, so would not have a document to prove age.

It is also worth mentioning that the UK's BBFC acting as an age verification regulator has approved this technology. The Age-verification Certificate (AVC) is a voluntary, non-statutory certification scheme to ensure age-verification providers maintain high standards of privacy

---

3 https://www.electoralcommission.org.uk/__data/assets/pdf_file/0004/194719/Proof-of-identity-scheme-updated-March-2016.pdf

and data security. The link to certification is available here: https://www.ageverificationregulator.com/av-certification

Yoti has also been asked to serve on the SHERPA Stakeholder Board, looking at the ethical dimensions of Smart Information Systems; formed to gather their views on existing threats, risks and possible solutions to achieve a better balance between the potential benefits of the new technologies and their impact on ethics and human rights.

> In the case of the use of Yoti outside of the app, a photo of the individual is analysed by Yoti with no other identifying information, and the algorithm decides whether this person is over a certain age threshold. The photo of the individual is deleted and not further stored.
>
> But how did Yoti train its algorithm? As outlined in Yoti's white paper on the Age Scan, data to train their algorithm is from three sources: data from Yoti users, from a dataset that they claim is "open-source" and licensed for commercial use, and photos of people in Nairobi, Kenya.

Yoti comment: the wording relating to the open-source database is misleading. As previously communicated to you we used the APPA-Real database in accordance with its terms. Before we used it we took legal advice from a leading London IP specialist law firm who confirmed we could use the database to train the algorithm. The APPA-Real database is well under 1% of our total dataset.

Please note you have put quote marks around 'open source' as though you are quoting from the Age Scan white paper. However, in that paper it says 'public domain source'.

We have carried out volunteer data collection activities, with clear consent, in the UK and Kenya.

> *In relation to data from Yoti users, if you have downloaded the Yoti app, at the point you add your verified identity document and it is accepted, your data becomes part of the training dataset. Specifically, this includes the year of birth and gender taken from your verified identity document; your 'selfie' photo taken when you set up the account; and Yoti researchers add other tags/ attributes for example by tagging skin colour. As of July 2019, Yoti had data of over 72,000 users that they were using to build and test their model. Yoti have told us that this data is held on a separate R&D server, where it is not stored with data like the name of the user.*
>
> *Privacy International have engaged with Yoti and raised concerns about Yoti's actions when we met in person. This includes:*
> - *At the point an individual has a verified ID document on their Yoti account, they are added to the training dataset. Yet once you have a verified ID document linked to the Yoti App, not only would you have no need to use Age Scan within the App, there are a vanishingly small number of scenarios when you would need to use Age Scan to prove your age when buying age restricted goods. This is because you can simply show the retailer your verified age in the App.*

Yoti comment: we addressed this point in our meeting with you. Your view is based on the premise that it is only valid to use a person's data where that person has a direct benefit. We dispute this assertion as data is frequently used to develop things that benefit society and individuals in general even if each specific individual whose data was used does not receive a direct benefit. The most obvious examples are in relation to research in medicine, social care, social policy, poverty and access to social justice.

Yoti is currently offering support, on a pro-bono basis, to an EPSRC project "Interaction Design for Trusted Sharing of Personal Health Data to Live Well with HIV". Our contribution focuses on allowing anonymity and pseudonymity.
https://gow.epsrc.ukri.org/NGBOViewGrant.aspx?GrantRef=EP/R033900/1

The Yoti platform is designed to help those with and without an ID document. In the case of Age Scan, as we set out in our meeting, individuals with an ID document on their Yoti **do** in fact benefit from the technology, given its use cases of proving age anonymously at self-checkouts for age-restricted products, or to anonymously access age-restricted content online. It is clearly incorrect to assert users have no use for Age Scan if they have an ID document in their Yoti. This option is open to everyone. If an individual wishes to buy an age-restricted good at a self-service checkout, without taking their phone out, or if they do not have their phone on them, they could use the Yoti age estimation. Some people may also choose to age estimate online to access an age-gated service, **even if they have an over-18 attribute verified from a document.**

- *At the time that Privacy International spoke to Yoti, their July 2019 Privacy Policy lacked transparency as to the use of Yoti user's data for the purposes of age verification, and the quality of information provided was poor. There was little clarity as to how the users' data was used as part of the Age Scan dataset. They have made improvements to their Privacy Policy following our conversation.*
- *In adding Yoti user's data to a training dataset used to train age verification technology, Yoti were using their customer's 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.*

Yoti comment: PI is entitled to hold a different opinion and it should be clear that the statements in these paragraphs are PI's opinion. We dispute the statements about poor quality information, reasonable expectations, fairness and purpose limitation. We maintain that we provide suitable transparency during onboarding as well as in the detailed privacy notice and in doing so we do not accept that the data uses are beyond the reasonable expectation of users. The R&D work provides the technology features in the app so we dispute there is any purpose limitation issue.
We recommend that you go through the onboarding process in the app, to go through the same experience as a user.

In addition, in 2019 we have worked with a number of bodies (World Privacy Forum , Centre for Democracy & Technology and IEEE expert Dr Allison Gardner) to carry out a review of our approach. We have also run roundtables inviting representatives from the ICO, Consumers International, Nesta, Responsible 100, Yo-Da, University of Warwick and Home Office Biometrics Ethics Committee, Consultant data, privacy and biometrics for CDT, Fabian Society, Gemserv, Centre for Data Ethics and Innovation, techUK, 5 rights, Unicef,

GCHQ/Vivace, Childrens Commissioner, NSPCC, Centre for Data Ethics & Innovation, Barnardos, and Doteveryone.

[redacted] of Privacy International were invited to the first of these which took place on 7 Jan 2019, but they declined to attend.

- *There is currently no accessible way for Yoti users to opt out of use of their data in the training dataset and no accessible way for Yoti App users to request that their data is deleted from the training set without stopping them being able to use the app altogether. Yoti have told us that they will implement a way for users to have a more granular opt-out; hopefully, this will be prompted at first use so that a user does not have to have their data included in the research dataset automatically, indeed an opt-in would be a better solution.*

Yoti comment: the opt-out from R&D use of data has been live in the app since the September app release. Users are informed of this on the biometric screens at onboarding. PI are entitled to their views as regards opt in.

Since talking to Privacy International, Yoti have made welcome improvements to their privacy policy, which have gone some way to making it some degree clearer the use to which they're putting a user's photo and passport data.

Yoti comment: for your information the latest app privacy notice dates from September, which includes the information about the R&D opt out. Yoti invites scrutiny from a wide number of academic, regulators and civil society organisations; as outlined in our blog about the roundtables conducted and through the various organisations we engage with including techUK, the Digital Policy Alliance, Age Verification Providers Association.

*As noted above, Yoti state they are working on an opt out for research and development use of their customers data, although there is currently no opt out option and we consider that in any event an opt-in basis would be preferable.*
*Yoti comment: as set out above, there is now an opt-out option.*

*We would encourage Yoti to actively contact all customers whose data formed part of the training dataset to ensure they are aware of how their data has been used. We do not believe that the more than 70,000 users whose data has been used to train the algorithm were adequately informed about the use of their photographs and data from their passport or other identity document.*

Yoti comment: we are surprised by this paragraph given our meeting and its explanation about the Yoti app as well as our privacy notice make very clear that we deliberately have no access to individual user data and have no way to contact users. Whilst we can include messaging to those signing in to our app we cannot, for example, email them.

We are reviewing plans to include a tile in the 'Discover' area of the app explaining how we use R&D training to protect Yoti app users and individuals who wish to use Yoti-powered tech outside of the Yoti app from harm. Harm includes the risk of fraud and the increased risk of loss of ID documents.

*There remains a core issue with Yoti's use of data gathered in the course of their identity work: how do we want the identity industry to treat our data? What is the*

*future for this market, and how do we limit what these companies are doing with the data they gather in the course of their operations?*

Yoti comment: We are surprised at the tone of your review; given that Yoti a company set up with privacy and security as core business principles. Yoti is proving to companies that you can be innovative and successful while also respecting privacy.

Yoti is purposefully designed to be consumer-centric and a privacy-friendly way to prove identity / age. Yoti is free to individuals. Businesses pay small and transparent fees to enable their customers to sign up or sign in more securely with less data.

We refer you to the Yoti Principles. A user chooses to set up their digital identity and chooses when to use it. The Yoti app is designed to provide higher and better security and fraud prevention.

Yoti cannot develop its privacy-friendly identity platform, its high-level security and fraud prevention technology without data. That is the purpose of the R&D work - this is a long way from the data use of other companies whose aims are to create vast databases for sale. Yoti does not operate an advertising business model of reselling consumer data; it is architected precisely to not be a relational database and so not to know what any individual does on a day-to-day basis. Our business model is to charge an organisation for a check and only when a consumer agrees to that data share.

*The future of digital identity*

As we look towards the future of a digital identity market, then we cannot allow it to develop into one where players profit from the exploitation of the data of its users.

Yoti comment: We would encourage PI to read the report by Future Agenda on the Future of Digital Identity"
"*The Digital ID landscape today is somewhat fractured with a variety of different stakeholders approaching the technology with different aims and different hopes. These varying perspectives on Digital ID are provided by (among others): National ID providers, the growing attempts to develop solutions based on international financial mechanisms and the organisations that underpin these, supra-national voices such as GSMA, The World Bank and the UN, and independent developers and funders such as, Yoti or the Omidyar Network. How these groups wield power and influence in coming months and years, and the successes they are able to attract, will have great bearing on the future direction and development of Digital ID systems.*"

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.

As outlined, in several instances above, the Yoti platform is architected as a non-relational database, the private key is given to the individual, in the secure module of their device. Hence if you are writing a blog piece about Yoti, this is not the case. If you are writing a separate blog piece on the wider market, we could understand why this point could be valid.

We would encourage the blog authors to look at existing market studies such as The Future of Digital Identities by Future Agenda, or recent Gartner studies. There are many digital identity companies that do not have a clear ethical framework, internal and external ethics boards or are not constituted as a BCorps.

PI Questions for clarification: response requested by 21 October

*1. In your privacy policy you state that you tag 'ethnicity'. You also refer to tagging skin tone. You rely on legitimate interests to process the data collected for the training dataset and used to train the Age Scan technology. According to Article 9(1) of the General Data Protection Regulation (GDPR), ethnicity is special category data and is prohibited unless you fulfil a condition in Article 9(2) of the GDPR or a condition in Schedule 1 of the Data Protection Act 2018. We consider that this means you would require explicit consent to process. On what basis do you believe you can rely on legitimate interests to process ethnicity data?*

Yoti response: the reference to 'ethnicity' is an error that had not been picked up and the text should only reference 'skin tone'. We use the Fitzpatrick scale to assign a skin tone to an image so that we can report on the algorithm's performance against different skin tones, so we can evidence the diversity of our training data set, and so we can determine if any group is under-represented. This aligns with our signature of the Safe Face Pledge. This data is not used to train the algorithm. The DPO will correct this error in the next app privacy notice update.

*2. You rely on legitimate interests to process data that forms the training dataset. Specifically, 'fraud', by which we understand you mean wider societal fraud in relation to age verification. We would be grateful for a copy of your legitimate interests' assessment.*

Yoti response: as I am sure you are aware, legitimate interests assessments are an internal company-confidential document. We do not make them publicly available, nor do we disclose them to third parties other than in response to a regulator request.

*3. When do you intend to offer an opt-out for new and existing Yoti users in relation to training and development? Will new users be given the opportunity to opt-out prior to their data being used in the Yoti Age Scan dataset? Furthermore, why do you consider it appropriate to provide an 'opt-out' rather than opt-in? In considering this, how have you taken into account your data protection by design and by default obligation in Article 25 of the GDPR?*

Yoti response: This opt out has been live in the app from the September app release. Users are informed of this in the biometric app screens.

We submitted our Age Scan technology and certain applications of it to the first round of the ICO Sandbox, but were not accepted. We will resubmit it once they start accepting new applications.

Age Scan is an example of privacy by design in that it allows anonymous age estimation and has been certified by the BBFC as an age-verification provider for companies subject to the Digital Economy Act's age-check provisions.

*4. Will it be possible for existing Yoti users, whose data forms part of the training dataset, to request their data be deleted, without having to close their account?*

Yoti response: Yes. As set out elsewhere, any user can go to the app settings at any time and opt out of R&D use of their data. This prevents further data from that user being sent to R&D, and it deletes all the data associated with that user that is on the R&D server and available for R&D to use. We have chosen to automatically delete the existing data when a user opts out or deletes their account, even though we do not legally have to under the research provision in GDPR article 17(3)(d).
Note: we use a privacy-by-design approach (hashed numbering) so that although we can find data of a specific user to action the data deletion, there is no way to get back to a specific user from the R&D data.