Yoti Guardians Council Meeting
22 October 2019

Attendance: See Table at end
Date: 22 October 2020, 1700-1930 GMT

Location: Yoti Office & VC
Recorder: Eric Levine

Agenda	1. Framing and current public dialogue on facial recognition technology and biometric data 2. Applying Ethical Framework to access control use cases	3. Feedback on Yoti's Ethical Framework process
Actions from Previous Meeting & this Meeting:		**Status Update**
○ Confirmation of Seyi Akiwowo as new Guardian Council member		Completed

Summary notes from the meeting are provided below, with points of agreement and actions clearly noted.

Welcome	The format of this Guardian Council meeting was adapted to more of a workshop structure for the majority of the meeting, looking at some of the privacy issues that have been prominent in public discourse, areas where Yoti has been pushed by civil society partners, and potential Yoti use cases that involve related complex privacy issues. Meeting began at 1700.
1. Framing and current public dialogue on facial recognition technology and biometric data	**Summary of Discussion:** Meeting opened with some initial framing discussion on issues related to privacy that are looming large in public dialogue and current events. Summary of this session includes: ● We are all aware there is an increasing amount of public dialogue, and some reactions from government and companies, around privacy issues related to facial recognition and biometric data being used for surveillance purposes. A few of the most public examples that were mentioned: ○ Public blow-up around a facial recognition surveillance scheme operating through CCTV cameras on the Kings Cross development site in Central London, which involved tracking individuals without their consent and police sharing facial images of a small number of individuals with the site owners for the purposes of facial identification. Public response to the news of this resulted in the site owner removing the facial recognition capability and promising not to introduce it in the future. Similarly, there has been a public push back from some police forces in the UK on UK Home Office efforts to pilot live facial recognition surveillance technologies more broadly in the UK. ○ In the US, one of Yoti's key markets, there has been a number of public stories of push back on the use of facial recognition technologies, with Apple, Microsoft and Amazon all involved in critical stories around the use of facial recognition tech. Earlier this year, San Francisco became the first American city to ban its agencies from using facial-recognition systems, and a handful of other medium sized cities have followed suit. ○ Further afield, but very high profile in the news, has been facial recognition for surveillance in Hong Kong during the protests there over the past few months, with protesters using umbrellas and masks to hide their faces, and at times tearing down facial recognition towers and cameras.

While in all these cases, the facial recognition technology is being used by governments and companies in very different contexts and for very different purposes than Yoti operates, the public dialogue around facial recognition technology has certainly escalated. This makes it easy for critiques of facial recognition technology to lump all facial recognition technology together and could make it harder for ethical businesses like Yoti to differentiate itself in the marketplace (or to have to spend significant attention in a defensive posture). It also makes it even more important for Yoti to think through the different ways that our technology can and should be used, and how to communicate most effectively on what we offer and why we have made the choices we have made to protect individual privacy.

- In addition to this public dialogue, Guardians also discussed the recent article and back and forth communication between Yoti and Privacy International. Summary of discussion on this exchange for Yoti to consider as it navigates this pioneering territory:
    - It is easy to present all facial recognition technologies and use of biometric data as a loss of individual privacy and control.
    - Given the loud public dialogue on these issues, and the number of actors who are taking a less ethical, individual-centred approach, it is easy to play on fears (in many cases justifiable) that individual’s data is/will be used for purposes that they are not aware of/consenting to.
    - In a rapidly evolving space, it is easy to assert that harms will come to specific minority groups, lead to discrimination, policing of social norms, etc.
    - As identity is a multi-faceted concept, it is easy to muddle the distinctions between verification of specific identity attributes (like age) that do not allow for an individual to be ‘identified’, and other combinations of identity attributes (like name + face) which do allow individuals to be identified.
    - The Council encouraged Yoti to continue engaging openly with good faith actors who are seeking to help address the complex issues involved in the application of new technologies, inviting those critics to join Yoti in seeking to identify the right course of action in these pioneering areas.

- Guardians agreed that as Yoti grows and becomes more prominent, and the broader public dialogue continues, it is likely that Yoti will be encountering this complex territory more often and will be more likely to be on the receiving end of critique and/or confusion. Yoti will not be able to isolate itself from the ‘political’ discussion on these topics, and the Council recognises how difficult it is to bring the appropriate level of nuance into these public discussions.
- Given that, the Guardians agreed that it will be important for the Yoti team, with engagement from the Guardian Council where appropriate, to spend time discussing such topics, exploring emerging potential use cases for Yoti that touch on these issues, and striving to find effective ways to communicate the thoughtful, ethical approach to digital identity that Yoti is seeking to pioneer.
- Guardians encouraged Yoti to do more to get in front of the facial recognition topic, which Guardians see as quickly becoming one of the pivotal issues in both privacy and identity conversations.
- The Council recognises that Yoti does not have all the answers (and there are many unresolved challenges), but that Yoti should continue to communicate openly and publicly in the media, at events, directly with authorities, using all channels it has to show that it is doing the hard work and dealing with the issue first-hand and taking public stands against unethical uses of facial recognition.

	● While recognising that Yoti is an early stage business with limited resources to deploy against a long list of short-term priorities, the Council encouraged Yoti to stand unambiguously at the most privacy protecting and individual-driven (rather than "user-centric") edge of this topic.
2. Applying Ethical Framework to access control use cases	**Topic:** The Council used Yoti's Ethical Framework (which Yoti has developed for use to think through complex issues in a structured way) in a mini-workshop format to look at potential access control use cases where: a) the reason for access control is security or regulatory; and b) where the reason for access control is to provide a preferential service (from a Yoti business/organisational client to their customers). In both cases the example uses cases that were considered are hypothetical. Guardians were requested to feedback on the hypothetical use cases, and to help identify considerations that Yoti has not yet flagged through its Ethical Framework. Yoti can be integrated into existing access control management systems or used for new forms of access control. Because of our ability to remotely verify an identity, or an aspect of identity, Yoti's technology can lower the friction and improve accuracy of access control in premises with limited access. Guardians have discussed many such use cases in previous meetings (e.g., access control to pubs and night clubs using age verification) where it is straight forward how individuals are informed/aware of the use of Yoti to verify their identity/aspects of their identity, where there is clear consent by the individual (or another option to prove their identity if they choose not to use Yoti). The access control use cases we want to look at involve situations where we have less control regarding how individuals are informed and/or give consent/have other options if they do not wish to use Yoti (which are the circumstances that Yoti prefers). The hypothetical use cases considered in this session were: **1. Examples of Access control for security and regulatory purposes (hypothetical):** ● **Regulatory Purposes - betting shop access control for age:** Because of government regulations, betting shops are under a requirement to prevent underage citizens entering the shop. To meet this regulatory requirement, the betting shop installs Yoti Age Scan at the entrance, running through a customised CCTV camera. The faces of all potential customers are scanned. The camera can be set to run continuously or to only search for faces at predetermined intervals (for example, every three seconds). Where a potential customer is estimated as being underage by Yoti Age Scan, members of staff are able to find the individual and ask them for an additional form of ID. In order to prevent Yoti Age Scan estimating the age of individuals who have recently entered the betting shop, a mechanism is installed which recognises where an individual has previously entered the betting shop and has been estimated to be over age. This mechanism does not store any other information about the individual and resets after a set period of time, thereby never recognising individuals indefinitely. In this scenario, Yoti would not have control over the way in which the betting shop informs prospective customers that they will be subject to Yoti Age Scan (although can provide guidance on how to do that effectively). Also, in this scenario, potential customers cannot opt out of being age estimated as all individuals entering the premises would be age estimated. ● **Security Purposes - courier service access control for secure premises:** A courier service wants to improve the security where its employees are entering secure premises, such as managed offices. The courier service adopts Yoti as its identity verification solution, integrates Yoti with its existing data management systems, and mandates that all employees set up a Yoti. Yoti is then integrated into the access management system in the managed premises. If the employee is unwilling to create a Yoti, they will be unable to fulfil the responsibilities of their job, and therefore unlikely to be able to continue as an employee.

Summary of Discussion on above examples: The Council agreed that there are significant potential benefits to deploying Yoti in access control cases for security/regulatory purposes, as well as many challenges and risks that need to be considered before Yoti can deploy in such use cases with confidence. Summary notes from the discussion included:

- Potential Benefits of Yoti being deployed in such use cases:
    - Helping to address social exclusion by allowing people near age limits but with no ID to be able to prove age.
    - Data minimisation principles are valuable, requiring smallest amount of data needed.
    - Using biometric data without sharing biometrics.
    - Not retaining data is a privacy upholding benefit.
    - Increases physical security, more rigorous/higher standard verification process, ess risk of mistakes, increases protections against false IDs.
    - Efficient re-assessment process for individuals, and reduces pressure on employees to conduct ID verifications.
    - Could help with wider education of public about what data is ‘necessary’ to help support data minimisation.
- Potential Risks/Harms of Yoti being deployed in such use cases:
    - Yoti is not in control about how people are informed of the use of this technology and their participation in its use (as Yoti can not inspect every site).
    - Mandatory use of any technology (as in courier example) is a challenge as not fully free consent.
    - Companies could potentially maintain images/lie to Yoti and use data for other purposes/add to their consumer profiles in violation of Yoti terms and conditions.
    - Risks for people who for any reason are trying to protect their identity.
- Ways to be Transparent/Ensure Consent:
    - Yoti can explain all that it does to make sure that consent is gained and information is given in premises where Yoti is being used.
    - Make sure clear standards and guidelines for all business partners of Yoti to use in notification of consumers entering premises.
    - Deploy Yoti in controlled spaces where notification and consent can be done well, and be public about Yoti technology being used in such situations and rationale for doing.
- Considerations for Communicating to Yoti Community:
    - Get more input from marginalised groups to ensure Yoti approach considers those who are often poorly served by new applications of technology.
    - Set up a possible ‘whistleblower’ process that would allow anyone to notify Yoti if its technology was being used inappropriately, or without consent and proper notification.
    - Ensure focus on the important problems being solved for individuals (not just the commercial benefit for business partners). Cleary communicate the spectrum of use cases, and what Yoti does and what it does not do.
    - Include opportunity to seek damages to Yoti brand in contracts from any companies keeping images or using data in ways that contravene Yoti terms and conditions.
    - Keep clear distinctions in all communications between Yoti and other facial recognition technologies that are used without notification/consent and/or retain images/data.

2. Examples of Access control for the purpose of offering personalised services (hypothetical):

It is also possible for Yoti to be used for automatic recognition of individuals to allow a business or organisation to provide a personalised service without the individual having to share any further information. In these instances, all individuals receiving personalised services would have to decide

	(and consent) to share their details with the receiving organisation prior to arriving in a specified location (where their face would be scanned to identify them and trigger the personalised service). However, for a personalised service to be provide to some individuals, the business/organisation would have to scan all individuals at that location (in order to identify those receiving the personalised service). In such situations, there would be individuals who have not opted to take part in the personalised service who are having their faces scanned (as with Yoti Age Scan, once a face is scanned, the image is deleted and not stored). In such situations, Yoti's technology would be deployed in circumstances where we have no control of if/ how people are notified they are being scanned by Yoti's technology. There could also be concerns about Yoti's technology being used in combination with public authority or private sector watchlists. Hypothetical examples of such personalised services: ● **Bag drop at an airport:** An airline would receive advance passenger details when a passenger decides to share them, prior to flying. This would include a biometric template, and consenting passengers would be informed of this data being used to identify them to facilitate their bag drop process on arrival at the airport. There would be a camera at the bag drop at the airport, which scanned the faces of people arriving at it. The camera would match faces against a database of biometric templates, which have been shared by customers through Yoti, using Yoti's 1:1 facial recognition technology. The camera recognises a face that has been shared with it and populates the customer's details at the check in. In this scenario, all individuals arriving at bag drop would be scanned (in order to identify those passengers who have pre-registered and shared biometric data). ● **Hotels Loyalty Programme Members:** Members of a hotel's loyalty scheme are issued and can carry a Radio Frequency ID (RFID) loyalty card to identify them as priority customers on arrival at a hotel. However, many customers do not carry their loyalty cards. The hotel would like to implement facial recognition technology to provide a solution to identify priority customers (who wish to be identified) more effectively. Consent to this would be given during the loyalty programme enrolment process. In order to identify these pre-registered and consenting priority customers on arrival at a hotel, cameras would capture the faces of all individuals entering the hotel and would recognise members of the loyalty programme. The customer would then receive a personalised service at the reception. Similarly, when individuals entered a hotel restaurant, their face would be captured to allow members of the loyalty programme to be identified, who would then receive a personalised service. **Summary of Discussion on above examples:** The Council concluded that in this type of use case there are: a) limited significant benefits to the individual beyond convenience; b) meaningful risks of individuals being scanned without their consent; and c) limited ability of Yoti to be able to ensure signage/notification of the use of its technology in each premise. Therefore, the Guardian Council encourages Yoti to proceed with extreme caution in this category of use cases regarding personalized services to ensure they are consistent with Yoti's principles and commitments to the Yoti community. Further observations from the Council' discussion included the following suggested guidelines to use in determining the viability of potential use cases: ● When deployed for access control, Yoti should only be ever used to check if you are human, and if you meet a certain age threshold. ● Until an individual chooses to identify themselves, Yoti should not identify an individual. ● Always err on the side of openness. Any complex use cases such as these above should be explained on the Yoti website, including the rationale/benefits intended for individuals, the risks considered, rationale for proceeding with the use case.
3. Feedback on Yoti's	**Summary:** Guardians were invited to give feedback on the Ethical Framework as a tool/process (outline of steps and framework appended at the end of this minutes document), and any

Ethical Framework process	improvements that Yoti can make with the benefit of having just used it to structure the previous discussion of access control use cases. Guardians endorsed the current version of the Ethical Framework, and encouraged Yoti to refine the structure through use and testing in real situations.
Adjournment	The meeting was called to a close at 1930.

2019 Meeting Attendance									
Meeting Dates	11/2	7/5	16/7	22/10	Yoti Staff	11/2	7/5	16/7	22/10
Renata Avila	●	●	●	●	Robin Tombs	●	☒	●	●
Doc Searls	●	●	●	●	Julie Dawson	●	●	☒	●
Joyce Searls	●	●	●	●	Leanne Marshall	●	●	●	●
Gavin Starks	●	●	●	●	Eric Levine	●	●	●	●
Seyi Akiwowo	☒	☒	☒	●	John Abbott	●	●	☒	☒
					Sam Rowe	☒	●	●	●
					Emma Butler	☒	☒	●	☒

● = in attendance ○ = absent/ apologies ☒ = Not scheduled to attend

Reference: Steps and structure of the Yoti Ethical Framework are as follows:

Stage/Step	**Description**
Recognising the ethical issue(s)	
What is the ethical issue?	Give a brief description of: a) the project that has given rise to the issue; b) the issue itself.
What relevant laws or regulations impact on the issue?	Think in particular about data protection and human rights including non-binding international frameworks and relevant codes of conduct
What relevant Yoti business principles impact on the issue?	Identify how the issue conflicts (or could conflict) with business principles and to what extent.
What Yoti public commitments or statements impact this issue?	For example, the Safe Face Pledge, public statements on the topic by senior management.
Recognising what might happen due to the issue(s)	
What are the relevant outcomes / risks?	What are the consequences of this issue - of inaction and action.
What public considerations might the ethical issue cause?	How may the press, the public or specific interest groups react to the issue.
What positive impacts could the project have on people?	What are the benefits of the project - what are the direct or unintended benefits?
What negative impacts could the project have on people?	What disadvantages or downsides have caused an ethical issue. These might be direct or unintended consequences.
What is the commercial impact?	Think about risks to current and future partners / commercial offerings & relationships.
Dealing with the issue	
How could we maximise benefits and minimise any negative impact?	What concrete steps, internal changes or external pressure can be made?
What relevant ethical frameworks can be applied to the issue?	These may be sector-specific frameworks or more general frameworks.
Should we engage with the public, NGOs or other experts on this matter?	It might be useful to talk to the public or other stakeholders about this issue, to get feedback.
If we should engage externally, when and how?	

Should we engage with our staff on this matter?	Which other staff should we engage, how and when?
Should we be talking publicly about this issue?	It will be appropriate to be transparent about some issues and not others.
Internal actions	
What actions need to be taken	Actions include getting further input; carrying out further research; making a recommendation to senior management; informing the Guardian Council; etc.
If an action needs to be taken on this issue, who will lead?	
If actions to be taken on this issue, who will review?	
Action plan	Set out the action points, who is responsible for them and deadlines.