Yoti Founding Guardians Council Meeting
6 July 2016

Attendance: See Table at end   **Location:** Yoti Office & VC   **Date:** 6 July 2016, 1700-1900 GMT   **Recorder:** Eric Levine

Agenda	1. Updates from last meeting. 2. Yoti product/business update 3. Topics for discussion with Guardians	4. Input on Social Partnerships Strategy 5. Input on Briefing Paper for No. 10 Downing Street 6. FYI - occupational requirements for Yoti staff

Carry Over Actions from Past Meetings:	Status Update
o Signing up to UN Guidelines on Businesses and Human Rights: Renata to inquire through UN contacts what the best way is for Yoti to engage with the UN towards publicly committing to the Guidelines, and Eric to work with Chris to include Yoti publicly committing to UN Guidelines in public communications planning when we get to public launch.	TBD with public launch
o Privacy Policy and Terms & Conditions: Ana coordinating process of discussing revised drafts of policies with Yoti legal counsel to negotiate changes to text of policy documents, and for Privacy Policy draft to be reviewed by new Data Protection hire, with revised documentation to be shared with Guardians when redrafted.	TBD in August

Actions from this Meeting:	Status Update
o Yoti's Go-to-Market Plan: Yoti doing research on programmatic advertising routes and trying to find routes that are respectful for potential users. Yoti will conduct small sample programmatic tests and will bring back results to Guardians for discussion. Whatever decisions are taken on advertising routes, Yoti will be fully transparent on choices.	Early September
o Yoti's Launch Marketing Plan: Joyce and Doc to source contacts for Chris on experts in non-programmatic advertising.	End-August
o Product Update: Paco to share report from Cigital pen testing with Guardians.	End-July
o Mandating Yotis: Renata to source a legal contact for Yoti on labour privacy issues.	End-August
o Criminal Use of Yoti: Yoti Senior Management Team to draft specific scenarios which support taking/not taking action to revoke an individual's use of Yoti for consideration (including clarifications of the types of crimes that Yoti would consider taking action on).	End-August
o Criminal Use of Yoti: Julie to solicit input from Yoti staff, potential users and a wide demographic of stakeholders regarding the issues raised and scenarios, gathering input for consideration to inform policy decisions.	End-October
o Criminal Use of Yoti: Ana to seek legal advice on Yoti's responsibilities to respond to information about Yoti being used to commit a crime, and the legal standing of Yoti's abusive conditions definition in the draft Terms & Conditions for consideration.	End-September
o Julie to lead on developing policy for reporting of suspected fraud at registration stage (both adults and minors to be covered), and policy for requests of information from third parties.	End-October
o Social Partnerships Strategy: Ken to meet with Eric, Chris, Chris and Julie to take forward the social partnerships strategy process, with output being shared with all Guardians.	Mid-September

Next Council Meeting	Next Council meeting: 18 October 2016, 1700-1930 UK time

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

Welcome	Meeting began at 1600, and Eric opened the meeting with a thank you to Guardians for their time and inputs on priority issues in between Council meetings, including introductions to privacy focused civil society meetings, introductions to DFID's Digital Innovation Team, and reviewing drafts of Yoti's Privacy Policy and Terms & Conditions.
1. Update on Actions from Past Meetings	Actions from past meetings that have been completed: ✔ Renata sent through consent models that have been developed and tested by Consumers International to inform revisions to how Yoti is asking users to consent to policies. ✔ Sub-group of Renata, Joyce, Doc, Ana and Duncan met to continue discussion on Terms & Conditions and Privacy Policy text, seeking to achieve a higher bar in how Yoti will fight for its users in these key policy documents. General feedback is that Guardians are satisfied with Yoti's intention to properly represent our users' interests (showing good faith), and recognise that we are breaking new ground and have to negotiate with legal counsel to agree acceptable final versions for launch that also balance liability issues for Yoti. ✔ Ana briefed David G and Bruce N before they attended Vendor Relationship Management Day as part of the Internet Identity Workshop in Mountain View. ✔ Julie confirmed that Yoti has discretion in sharing any 'matches' of known illegal identities that appear in the Yoti registration process with document authorities. ✔ Joyce and Doc had follow-up meeting with Chris and Robin on Launch Marketing Plan, with conclusions to be shared with all Guardians. Actions from past meetings discussed in this meeting: o Yoti's Launch Marketing Plan: Yoti doing research on programmatic advertising routes and trying to find routes that are respectful for potential users. Yoti will conduct small sample programmatic tests and will bring back results to Guardians for discussion. Whatever decisions are taken on advertising routes, Yoti will be fully transparent on choices. Action from past meetings still outstanding: o Signing up to UN Guidelines on Businesses and Human Rights: Robin and Duncan attended ID2020 Conference, and Yoti confident that we can make a significant contribution to Sustainable Development Goal 16.9 to address global identity issues, although not yet sure exactly how we can best engage with other actors – any contacts in this space very welcome from Guardians. Renata to inquire through UN contacts what the best way is for Yoti to engage with the UN towards publicly committing to the Guidelines, and Eric to work with Chris to include Yoti publicly committing to UN Guidelines in public communications planning when we get to public launch. o Privacy Policy and Terms & Conditions: Ana coordinating process of discussing revised drafts of policies with Yoti legal counsel to negotiate changes to text of policy documents, and for Privacy Policy draft to be reviewed by new Data Protection hire, with revised documentation to be shared with Guardians when redrafted.
2. Yoti Product Update	Paco summarised good progress being made on product through the key milestones of our technical build and launch plan. The most recent release – R6 – is scheduled to go live on 18 July 2016. This version will be used in Yoti's first full external pilots with a range of first mover potential clients in the public, private and civil society sectors. We currently have a strong selection of businesses, organisations and institutions who have requested pilots with the release of R6 – in areas ranging from private and charity sector recruitment, night club age verification, online gaming, online classifieds, and more. We will now be re-engaging with these interested parties to determine which will form the portfolio of external pilots to undertake over the next few months. Paco also summarised penetration testing that was conducted with Cigital, as well as less traditional pen testing with Hacker House. All pen testing has been successful from Yoti's perspective, with no major issues being discovered in either black box or white box tests. Minor issues flagged by Cigital in the white box tests have already been addressed.

	Yoti also received the 'Cyber Security Start-up of the Year' award at the 2016 Cyber Security Awards. **Actions:** o End-July: Paco to share report from Cigital pen testing with Guardians.
3. Discussion Topics	The following three points were complex issues which have emerged as we have considered in more detail the implications of Yoti's public launch and work with different potential clients/user communities that were tabled for input and advice from Guardians.
3a. Mandating Yotis	<u>Issue:</u> It is easy to see that when Yoti provides an efficient service for a client (e.g., using a Yoti to authenticate entry into a building or any other seemingly innocuous Yoti-assisted activity), the result could be that an individual employee/volunteer of that client would be mandated to have a Yoti or accept a Yoti attribute to fulfil their job or voluntary role. Yoti is not in the business of 'forcing' individuals to have or use Yotis, and this seems in some way to be contrary to our pledges and promises around user control and choice. One way of addressing this would be for Yoti to insist/request that all clients who offer a Yoti attribute, also offer another route to achieve the same goal (e.g, individual should be able to show ID card or passport to enter a building, scout leader should have the option to carry or show paper copies of first aid, Disclosure and Barring Service certificates, etc.). On one hand, we think that it may not be realistically within our mandate to insist/request that clients offer an alternative, as could be taken as interference in their organisational structures and culture (but could vary from sector to sector, perhaps depending on whether there has recently been a 'paper' alternative that has been replaced). On the other hand, as one of Yoti's main benefits is providing a more robust way of detecting fraud, then it would be wrong to insist that a client operate an alternative path, if that path is inherently more prone to fraud/spoofing. <u>Question:</u> Is this a legitimate civil liberties issue that we should be considering and developing a range of responses/solutions for? Is this beyond our mandate and therefore not up to Yoti to insist/suggest alternatives to clients? Any advice welcome on how we approach this. In discussing this matter, <u>points of agreement</u> included: • Businesses and organisations decide what technology their employees need to use. • This is an organisational decision, not Yoti's decision (similar to organisations choosing pension plans, health insurance, and other areas on behalf of their employees). • Yoti is making interactions more secure, and increasing privacy for users, and so not compromising security or privacy for any employees who are required to use Yotis. • Yoti allows organisations who know their employees / members to request use of Yoti (selfie tied to mobile phone only, with employees accepting an organisational attribute). Many organisations will not need to require that the Yoti must be anchored by a government photo ID, and employees can decide to add a government photo ID if they think it will make Yoti more useful for them personally – so individual employees would retain a large degree of choice in what information they want to upload to their Yoti. **Actions:** o Renata to source a legal contact for Yoti on labour privacy issues.
3b. Individuals Convicted of Crimes that Involve Using Yotis	<u>Issue:</u> We are considering whether Yoti should have a policy regarding use of Yoti by individuals who exploit Yoti in the commission of a serious crime (that has been tried and convicted), and whether Yoti should take steps to remove a user's access to their Yoti to prevent any potential future harm. On the one hand, Yoti is an identity and attribute system, not a reputation system. However, given the levels of verification of certain attributes it is likely that some users of Yoti will see Yoti sharers of info to be more trustworthy (as there is more trust in a handshake with biometrics and audit trail), which could lead to Yoti being perceived as a reputation system.

Yoti can show which evidence sources uphold that someone is who they say they are, but no identity provider can give 100% certainty that a person is who they say they are. If a criminal wants to use Yoti, identifying themselves each time, they are likely to get caught and incarcerated if the crimes are serious (without Yoti getting involved). It is also definitely more practical for Yoti not to get involved in suspending (for a long time or permanently) someone's use of Yoti.

On the other hand, it could be perceived that we are not necessarily protecting our user community if we allow someone who has shown that they will exploit the 'trust' implied by using a Yoti to commit a serious crime, to continue to use our service.

Questions: Should Yoti in exceptional circumstances prevent a user, who has exploited Yoti and caused serious harm to another individual, from continuing to use Yoti? If there are exceptional circumstances in which Yoti should prevent a person from using a Yoti, how do we define what those circumstances are? If we do think that we should play a more active role in protecting our user community and the 'trust' provided by using a Yoti, should we also respond to the Police, if they have Court evidence that a person who has used Yoti as part of an event path to commit a crime, if they request we deny that person the use of Yoti?

In discussing this matter, points of agreement included:
- We recognised that this is a difficult area and we need to carefully consider the complications and nuances on both sides of the argument.
- All technologies, regardless of how they are originally intended to be used, can be used in malicious ways – and we need to expect this with Yoti's system. Use of Yoti leaving a clear biometric audit trail should be a deterrent to committing a crime; there does however remain a risk that people may manipulate the system.
- Yoti cannot accept responsibility for judging individuals who commit crimes that do not involve using Yoti (and will therefore not revoke the use of any individual's Yoti for any such reason).
- Yoti cannot accept responsibility for tracking publicly available information on its users (e.g. court judgements in every country where Yoti operates). Yoti can only respond to potential and convicted criminal acts when the legal authorities request data during the investigation of a crime, or when a court specifically communicates a mandate to Yoti following a conviction of a crime involving the use of Yoti.
- Yoti, in some instances, at the registration stage will have an obligation to report suspected fraud or counterfeiting or injection / combination attacks to various authorities and law enforcement bodies, which will vary by geography. This may lead to individuals being suspended or blocked from registering.
- Yoti will respect legal judgements and revoke an individual's use of Yoti where an individual is: a) convicted of a crime involving the use of a Yoti; AND b) the court communicates to Yoti a requirement to revoke that individual's use of Yoti.
- As per previous discussions regarding Yoti's commitment to uphold the UN Guidelines on Businesses and Human Rights, Yoti will not revoke an individual's use of Yoti in cases where a conviction is brought as a means of political persecution and violation of that individual's human rights (these cases will be reviewed on an individual basis in line with the UN Guidelines on Businesses and Human Rights by Yoti management and the Guardian Council).
- Yoti will verify data from our systems to law enforcement according to the approach laid out in Yoti Data Request Principles, Disclosure & Transparency Policy, when: a) legal warrants requesting verification of data as part of the formal investigation of a crime; AND b) the individual Yoti user who is the alleged victim of the crime willingly provides the receipts from the relevant Yoti transactions to the authorities, allowing Yoti to verify the validity of the receipt.
- Over time Yoti will need to evolve its policies in terms of approach to time limited suspension and time non limited blocking.
- We need to get legal counsel on criminal and human rights law on how to balance the right of a person to have a clean slate after they have finished serving a sentence for a crime, versus the rights of those using the platform.

In addition to the above points of agreement, the group held a lengthy discussion but did not reach agreement on how to handle situations when:

<table>
<tr>
<td></td>
<td>

a) An individual is convicted of a serious crime where they have exploited their Yoti to facilitate the crime in some way; AND

b) Yoti has been made aware of the crime via a request for evidence from the lawful authorities investigating the crime, or presenting evidence of the crime in a court process; AND

c) The court convicts the individual of the crime, but does not formally communicate to Yoti any mandate to revoke the individual's use of their Yoti.

The group recognised clear reasons why Yoti should consider revoking an individual's Yoti in these cases, including:

- Yoti as a business exists to build trust in the world by facilitating interactions between individuals who have been authenticated as unique, authentic persons by our system. However, if people can use Yoti with malicious intent, this will result in a loss of trust for other users in the Yoti ecosystem.
- Yoti's terms and conditions stipulate that users can not 'use or interact with our App in any unlawful or fraudulent way' and therefore Yoti should consider taking action to revoke an individual's use of Yoti if we are made aware that they have been convicted of using their Yoti in the commission of a serious crime (or use Yoti to facilitate in some way the commission of a serious crime).
- Yoti's users may expect us to act to revoke an individual's use of Yoti if we are aware that they have used Yoti with malicious intent.

The group also recognised clear reasons why Yoti should consider limiting it's actions in these cases and not revoking an individual's Yoti, including:

- Yoti can not make any guarantees regarding the intentions of any Yoti user – we can only guarantee that an individual using a Yoti is a legitimate, unique person, and the name, age and other authenticated attributes they share via Yoti have been verified.
- If Yoti was to take unilateral action to revoke any individual's Yoti, this could lead to users mistakenly concluding that Yoti somehow 'polices' its users and removes malicious actors (and by doing could lead individuals to fail to use appropriate caution when using Yoti's system).
- Yoti is not in a position to judge the intent of all of its users, and therefore must consider carefully whether we are in a position to unilaterally judge the intention of any of our users (without the mandate of a lawful court mandating Yoti to take action).

The group agreed to consider the issue again at a future meeting when progress has been made on the following the agreed action steps.

Actions:

o Yoti Senior Management Team to lead drafting of specific scenarios which support taking/not taking action to revoke an individual's use of Yoti for consideration (including clarifications of the types of serious crimes that Yoti would consider taking action on).

o Julie to solicit input from Yoti staff, potential users and a wide demographic of stakeholders regarding the issues raised and scenarios, gathering input for consideration to inform policy decisions.

o Ana to seek legal advice on Yoti's responsibilities to respond to information about Yoti being used to commit a crime, and the legal standing of Yoti's abusive conditions definition in the draft Terms & Conditions for consideration.

o Julie to lead on developing policy for reporting of suspected fraud at registration stage (both adults and minors to be covered), and policy for requests of information from third parties.

</td>
</tr>
<tr>
<td>

3c. Default Settings

</td>
<td>

<u>Issue:</u> Yoti is a promoter of data minimisation in general; however, we are considering the potential need/rationale for recording of 'anonymous' person-to-person Yoti transactions in case there is a future need to find out who the parties of the transaction were – e.g., if a person was killed or comatose after some transaction using a Yoti (e.g., meeting someone from a dating site) and the police (with a warrant) request the receipt to see who the other party to the transaction was.

One way of approaching this would be to set up a default setting for 'anonymous' peer-to-peer transactions (where the two parties have agreed not to share name), where the names and faces of the two persons in the transaction are stored in a secure 3rd party database (not Yoti). The 3rd party database could be controlled (and release of such receipts) by independent lawyers, an online safety charity, or some other objective ethical party serving as an appropriate custodian.

</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>

Or, if both parties choose to conduct an 'anonymous' person-to-person transaction (and opt out of such a default setting), we could warn them of the risk involved, and that Yoti will not be able to find this receipt without the private key held only by them.

Question: Is such a default setting and use of a 3rd party database for such 'anonymous' transactions, a valuable service to provide or an intrusion on the pledge we make to our users to leave them in control of their identity and data?

In discussing this matter, points of agreement included:
- Yoti would not be able to guarantee the conduct or exposure of a third party entrusted to hold Yoti receipts. As this would potentially compromise Yoti's ability to fulfill its promise to users, Yoti should not use a third party holding data for this functionality.
- Yoti should consider offering the ability for users to produce an additional receipt to be held by Yoti for anonymous person-to-person transactions where the parties involved want an additional receipt to be held in 'escrow,' that could be retrieved in the event that something goes wrong with the transaction (or if specific conditions agreed by both parties are met). This could be viewed as a valuable additional 'graduated disclosure' service by users, and is consistent with Yoti's principles around users being in control of their own identity and data.
- Yoti should only consider offering this additional service if it in no way compromises the security of Yoti's core systems

</td>
</tr>
<tr>
<td>

4. Social Partnerships Strategy

</td>
<td>

One of the central ambitions for Yoti (and unique aspects of our business model) is to provide a free digital ID service to social purpose organisations all around the world to contribute to the achievement of their social aims as well as supporting them to operate more efficiently/securely.

While we have had a range of meetings and discussions with a wide range of potential social purpose organisational partners (including some with whom we are exploring pilots using the R6 release), we have not yet done this under a clear strategic framework or categorisation of social 'verticals.' To date, we have been almost exclusively focused on the essential technology milestones of our product development roadmap, and the early stage business development efforts to ensure that Yoti has a good chance at becoming a sustainable company post-launch.

We now think that it is time to plan more formally and strategically how we approach the virtually infinite range of potential social partnerships we could pursue, and so have invited input, advice and suggestions from Guardians about how to approach this – e.g,:
- sectors that are particularly good 'fits' for Yoti
- thought leaders in the ID for social purpose space
- networks that Yoti should consider connecting with
- ways of inviting creative use of Yoti technology by social purpose organisations
- criteria for selecting social purpose partners
- possible areas of conflict with our promises and pledges to our user community

Informing our social partnerships planning, the basic types of functionality that Yoti will be able to provide in the short- to medium-term will be:
- **Biometric log-in** effectively means logging into a website or system without username or password (it does not require the backing of a government issued document)
- **Know Your Customer** (the ability of any organisation to 'know' a user via Yoti registration) will be rolled out in 3 stages: Passport will be very soon, Drivers Licence some way away, additional checks such as address or credit (through CallCredit) are somewhere between the two.
- **Peer-to-Peer** is the ability of any organisation to facilitate trustworthy ID/attribute sharing between individuals, remotely or face-to-face.
- **Additional Attributes/Badges** is the ability of any organisation to assign an attribute (or 'badge') to an individual's Yoti, providing a trustworthy certificate of an employment, skill, course completion, Disclosure and Barring Service check, or other attribute (that an individual can then share with others).

</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>

In terms of Yoti users being able to add government photo IDs to their Yoti profile, for launch we will be able to work with passports for the 110+ countries that issue chip passports. For Driving Licences, we will be restricted to UK versions for the initial public launch. Also, additional verification checks on addresses will be restricted to UK addresses for the initial public launch (through Call Credit).

In discussing this matter, <u>points of agreement</u> included:
- Yoti should consider conducting (or hiring a consultant to produce) a landscaping analysis of trends and actors in sectors where digital identity is/can be used for delivering social outcomes to inform our focus and efforts (e.g., last mile health service delivery, direct payments in humanitarian aid, etc.)
- Yoti should formalise responsibilities in the staff team regarding lead representation of Yoti in relevant Information and Communication Technology for Development (ICT4D), Tech 4 Good communities, to stay abreast of trends and identify potential partnerships.
- Yoti should consider how to invite and inspire creative ideas and applications of Yoti technology for social good from tech and social purpose sectors.
- Yoti should consider adopting specific thematic focus areas that the company will pro-actively seek and develop partnerships in to support social objectives (in addition to making our technology easy to access free of charge for all social purpose organisations). This should include consideration of Yoti applications in response to humanitarian emergencies.
- In the development and implementation of our social partnerships strategy, Yoti should engage staff (and eventually our user community) in the process wherever possible.
- Yoti wants to support the use of Yoti by social purpose organisations in:
  a. External: Ways that increase or improve the delivery of positive social outcomes (prevention of negative social outcomes) with partner organisation's 'beneficiaries'; and
  b. Internal: Allow social purpose organisations to gain operational efficiencies (repurposing applications which Yoti is developing for commercial clients), enabling resources to be redirected for delivering their social objectives.
- When developing new social purpose partnerships, Yoti should consider starting with 'internal' applications, as it will allow a social partner's staff to get familiar with using a new technology solution, increase their ability to effectively use and promote the use of Yoti in their work.
- When implementing our social partnerships strategy, the quality of social partnerships should take primary importance, rather than the quantity of partnerships.
- In the same way that Yoti is thoughtful about selecting commercial clients, we need to be equally careful in the selection of social partnerships and mindful of reputational risks.

Actions:
- Mid-September: Ken to meet with Eric, Chris, Chris and Julie to take forward the social partnerships strategy process, with output being shared with all Guardians.

</td>
</tr>
<tr>
<td>

5. Policy Briefing Paper

</td>
<td>

Following a number of positive meetings with different departments of the UK government around a range of potential Yoti use cases, Yoti was asked to present to a No. 10 Downing Street Policy Unit looking at blockages in the labour market and how things could be streamlined. Following the presentation, Yoti has been invited to contribute our thoughts on the positive role that digital ID could play in three broad areas:
1) Use cases where digital identity with improved access to government data would streamline data verification and processes.
2) Examples of where current regulation forces companies, etc to do things an 'old way' and prevents evolution to new, improved digital processes.
3) Example of where there is as yet no legislation, but where use of a digital identity could be for the public good.

Guardians were invited to contribute their expertise and suggestions as part of a paper Yoti is drafting to inform government policy makers in this area.

</td>
</tr>
<tr>
<td>

6. Staff Policies

</td>
<td>

Guardians were advised about a new Yoti operational policy matter, given the sensitive nature of the religious and cultural issues involved. Yoti will soon be moving to use a Yoti-based Admin system for employees to access systems and work in the secure environment of our clean room. This will require employees to be able to show their full face for biometric identification, as per passport guidelines. We have been given legal advice

</td>
</tr>
</table>

	that we should draft a neutrality policy statement that makes clear the occupational requirement (security nature and context of the employee's activity in the clean room), as well as stating that Yoti is neutral in relation to religious and cultural customs and norms of dress – to prevent any perception of discrimination from applicants and employees who practice a norm of dress that obscures their face.
Adjournment	The meeting was called to a close at 1830.

2016 Meeting Attendance													
Meeting Dates	12/1	6/4	6/7				Yoti Staff	12/1	6/4	6/7			
Ken Banks	●	●	●				Robin Tombs	●	●	●			
Renata Avila	●	●	●				Duncan Francis	●	●	●			
Doc Searls	●	●	●				Paco Garcia	●	●	●			
Joyce Searls	●	●	●				Chris Field	●	●	●			
							Ana Castanheira	●	●	●			
							Julie Dawson	◯	◯	●			
							Eric Levine	●	●	●			

● = in attendance   ◯ = absent/ apologies   ⊠ = Not scheduled to attend