Biometrics Focus Group Final Report

Report written by Maria Marlow, Senior Associate Consultant at BYC

Introduction

The Information Commissioner's Office (ICO) commissioned the British Youth Council (BYC) to recruit and deliver a focus group with 12 young people (between 15 and 17 years of age) on the topic of biometrics.

Information gathered from the focus group will be used to inform guidance for organisations around biometric use.

This report summarises that workshop, which was run in January 2023.

The following comments represent the views of participants in the workshop, and do not reflect the views of the ICO or BYC.

Structure of the workshop

The workshop took participants through the following exercises.

1. Defining biometrics
2. Case studies
3. Opportunities and concerns for use in Tech, leisure and education.
4. Scenarios
5. Thoughts on a Golden Standard for biometrics

Highlights

1. Young people were only really familiar with **biometric recognition** techniques, specifically fingerprint, face, voice and iris recognition.
2. Young people considered having control over there biometric data particularly important and expressed concerns about using that data to profile or compare people or their performance.
3. Before using a new biometric technology, young people wanted clarity on how it worked and where the data went.
4. Young people saw some opportunity for benefits when choosing how their biometric data is used.
5. Young people’s attitudes to using biometrics turned on whether it benefitted them and who used the data.
6. Any gold standard would involve being transparent about how biometrics are used, and using technology that meets recognised standards.

Defining biometrics

The group shared some of the biometric technology they had heard of and felt more familiar with. In order of **most known** to **least known** this is how they categorised the different biometrics:

- Fingerprint recognition
- Face recognition
- Voice recognition
- Iris recognition
- Heartbeat analysis
- Gait analysis
- Vein recognition
- Emotion recognition
- Keystroke analysis

They knew very little about anything below iris recognition and set about in pairs finding out more about each of these.

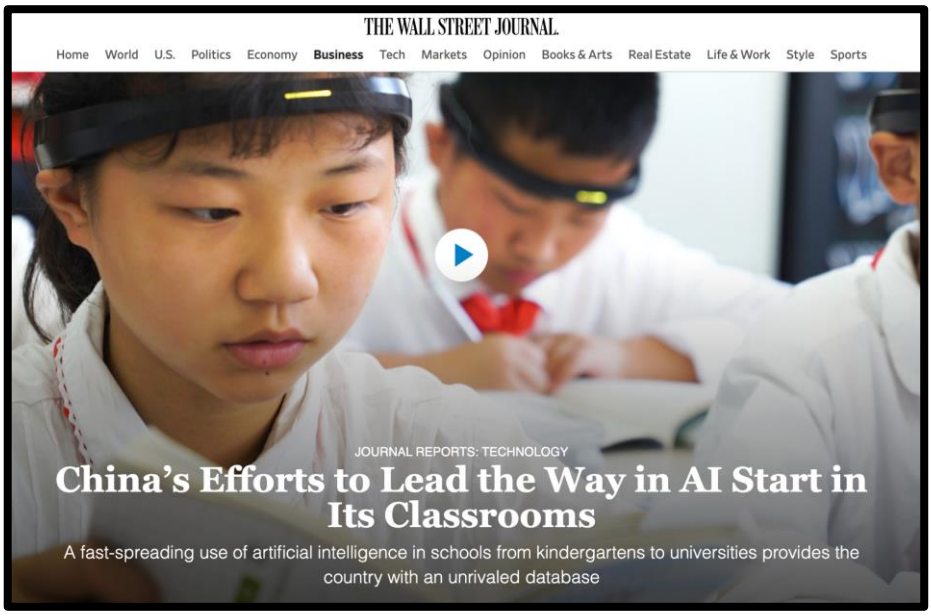
The sources they used to find this information were:

- Google
- Wikipedia
- Financial Times article
- News outlets
- Website - Cambridge Cognition (word Cambridge made them determine this was probably trustworthy)
- Cyber National Security
- FBI.gov (.gov deemed reliable source)
- Cambridge university
- Wired - interview with expert
- NHS website
- Forbes
- Centre for research and evidence on security threats
- Medical journals - peer reviewed
- The Medical
- Science direct
- Doctoral thesis
- ICO website

Case Studies

The groups then looked at three case studies and were asked to explore and discuss a series of questions. Below is a summary of the key points captured by facilitators who were sitting with the groups:

Case Study 1 - China's Efforts to Lead the Way in AI Start in Its Classrooms



Article Link: https://www.wsj.com/articles/chinas-efforts-to-lead-the-way-in-ai-start-in-its-classrooms-11571958181

Summary of Reflections

- Collecting data in order to be able to label or judge based on one data set felt unfair and the use of data in this way by schools felt like an infringement of their rights. It didn't leave any room for individual challenges a young person might be experiencing e.g. living in poverty, poor diet, poor sleep etc.
- Sharing data to a wider group e.g. parents of other children felt unnecessary and that it would lead to even greater comparison for the children.
- It was felt to be really important to have absolute authority over your own data, this felt to people what informed consent meant. Informed consent could only be given when there was clear information about how the data was being used. This must include potential negative impact of the data collection as well as positive.

- It was felt that you needed absolute transparency on what information (personal data) was being collected about you and where it was going.
- The ability to be able to opt out was seen as key, if you felt that the proposal had no real benefit to you.
- There should be the option to have your information deleted, or at least to request to have it deleted.
- Constant surveillance in any way should only be used where it is absolutely necessary from a safety perspective. The additional stress that could be caused by collecting data in this way could be significant.
- Data should only be collected where there is clear evidence or research that offers clarity about the success of such data being used and collected.
- Overall it was felt that using data in this way in the UK would be unacceptable.

Case Study 2 - Samsung S8 ‘eye security’ fooled by photo.

Article Link: https://www.bbc.co.uk/news/technology-40012990

Summary of Reflections:

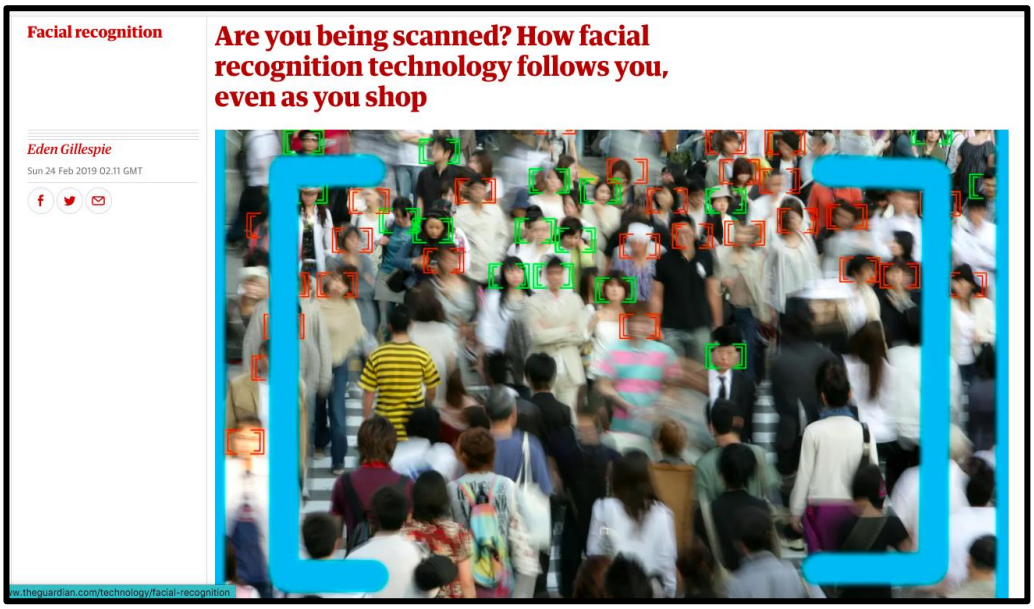
- It is important that biometrics and technology collecting biometric data is fully tested before coming to market. Should there be a standard that every company should meet before bringing a product to market?
- Our level of comfort with technologies changes as it becomes more mainstream. How can we make sure that young people have clear information about all new technologies as they are developed?
- Transparency of data collection remained a priority in this case study. How is this data being stored and used by the organisation that collects it?
- When we give consent to our data being used e.g. in a privacy policy this does not provide a clear and accessible form of information for young people about what is being collected and why. If you want to understand it, you need a level of education and understanding that not all young people might have. Developers should prioritise safety and transparency over profit.
- Company websites should provide more information about safety and how their authentication processes work.

- Greater education is important, and the curriculum should be constantly reviewed to reflect the fast-paced changes in this area.

When asked about what kind of things they would like to know before adopting a new biometric tech feature in this space, the group volunteered the following;

1. They would want to know where the data goes.
2. They would want to understand how the process works (a suggestion was made of a short video that explained it). When expanding on what this meant to them one delegate suggested they would want to know what made this better/ more secure than existing verification methods.
3. They would want some information on how spoofing could happen (so something here about security considerations and potential attack vectors – this is getting into what it would take for them to consider they could make an 'informed decision to decide to use it).
4. They would want information on how long the data is kept for.

Case Study 3 - Are you being scanned? How facial recognition technology follows you, even as you shop.



Article Link: https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop

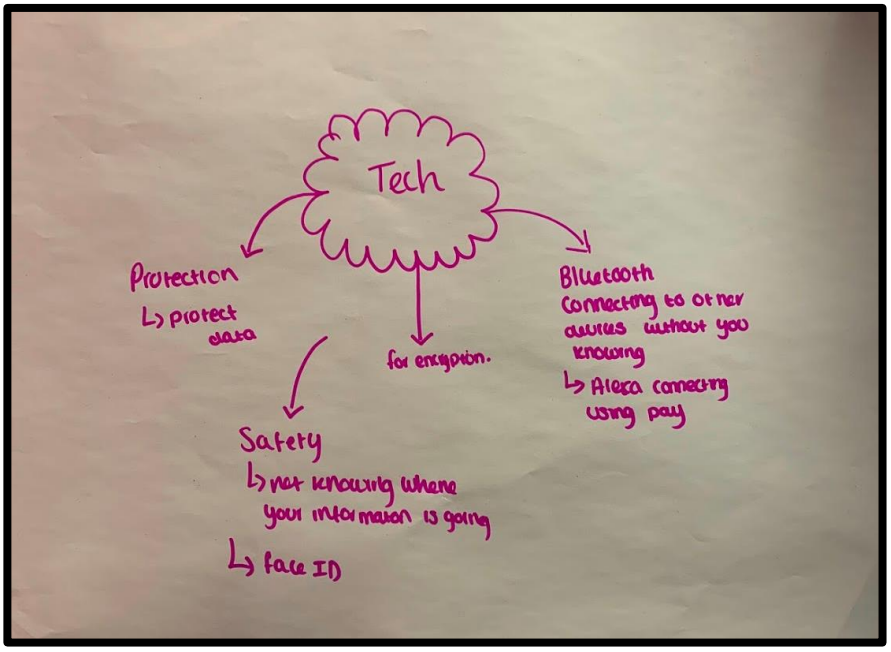
Summary of Reflections:

- In this example young people felt like their data was being used without their consent and that using data in this way was invasive and manipulative.
- This use case was seen very differently depending on who was doing it and why; young people were more likely to find this acceptable for public safety (finding missing children) and used by police v used by shops to monitor footfall or engagement with displays or stock.
- It needs to be clear that this data is collected, for what purpose, where else it is being used / shared etc.
- The group referred to a definite dividing line of when the processing ' is not in my favour' as when they would object to being tracked/advertised to in real life.
- Being presented with something *someone else suggested* all the time was also seen as a real life parallel to online advertising which could have the effect of feeling 'limiting,' and curtailing 'your ability to make choices about what you see.'
- Young people felt that this impacted their freedom.

Opportunities and concerns

After lunch, the group split into three to explore the use of biometrics in three areas. These were Tech e.g. banking, phones, computers, Leisure e.g. cinema, gym, shops and Education.

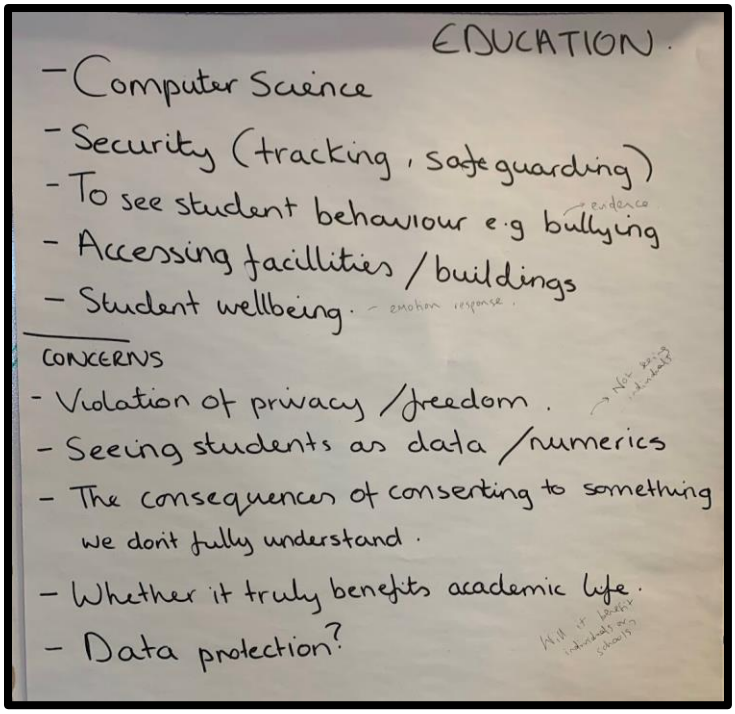
Technology



Summary of discussion:

- Important that any data used or collected by tech companies is protected.
- Young people wanted to know where the information they provide is going.
- Some value of biometrics in tech used to protect our safety.
- Some comfort around existing uses of biometrics that are used in this way.
- Better education needed about how data is used.

Education



Summary of discussion:

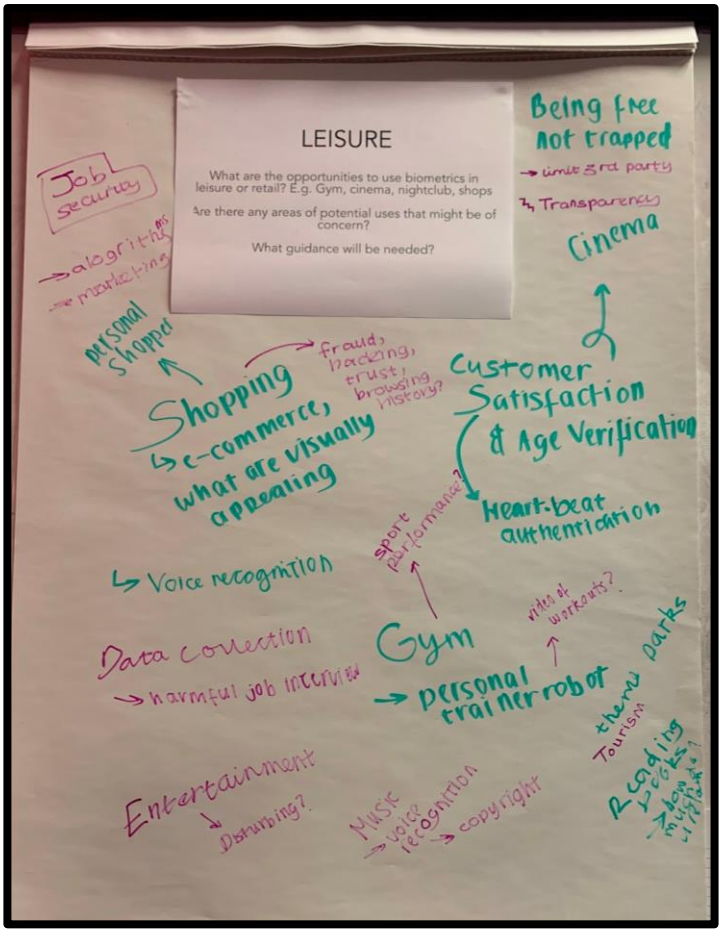
Opportunities:

- Could be useful if used to support students who experience discrimination or bullying to provide evidence of this.
- Helpful where it can improve ease of access.
- Emotion recognition might be able to track student wellbeing and put measures in place to support students early on where they are experiencing poor wellbeing.

Concerns

- May lead to a lack of individual support for students - grouping them by data or other metrics.
- Young people may not fully understand what they are consenting to - ethical implications of this.
- There is a lack of research about whether biometrics can actually improve things for young people. A lot more evidence would be needed to justify using biometrics in this way.

Leisure



Summary of discussion:

Opportunities:

- Gym – tracking with exercise, robots who help with workouts.
- Nightclubs – ID for age based on face. Also for security purpose
- Cinema: emotion detection eg heart rate detection, make films scarier based on reactions, age verification
- Shopping: personalisation, what is visually appealing, advertising, voice recognition online (eg for paying with Siri), personal shopper based on likes/dislikes.
- Voice recognition could help with copyrighting (?)
- Sports performances: Olympics training, using biometrics to improve performance.

Concerns:

By tracking people in their free time, do they have leisure?

Risk of fraud/hacking. Building a false sense of trust when emotion recognition is used. Also real-life tracking + online tracking means there is nowhere you are not tracked.

- Therapy: emotion recognition
- Deepfakes: facial recognition & voice recognition to trick people but also for entertainment (eg concert).
- Risks: data collection in your free time could be used against you. Eg leisure data used for job applications. Also risks of collection / hacking of data.

Should be able to choose if biometrics are used or not.

What guidance will be needed?

- Information needs to be secure.
- People also tick "I accept": imbalance. Easier to be "tricked" into saying yes online as compared to in person.

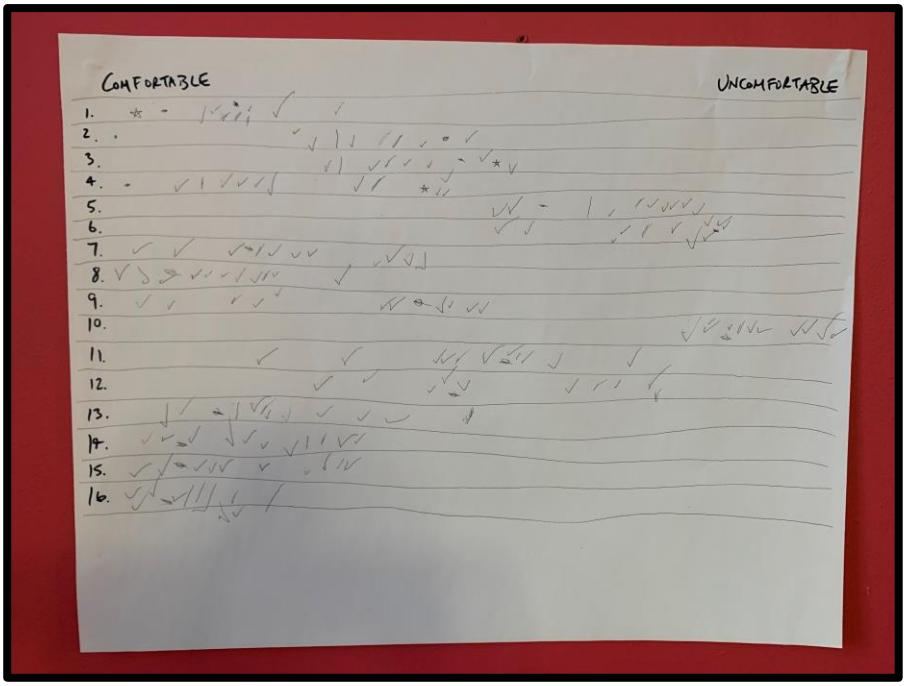
Concerns: job security for jobs that could be replaced.

Scenarios

The group then looked at 16 statements about the use of biometrics and rated their levels of comfort about the use.

Comments made when discussing each statement can be found below. Broadly the key points referenced were:

1. **What is the purpose of collecting the data?** The group broadly agreed that if it was for the safety of the user or society then that was an acceptable justification for gathering the information.
2. **How transparent is the organisation collecting the information about how they will use the data?** The group all want clarity when their data is collected about how their data will be used, stored and their rights in relation to it.
3. **Who is collecting the data?** Young people trust some organisations more than others e.g. police and school. This is also linked to the purpose of the data collection - as long as this was justifiable and for their safety then that felt more comfortable. Trusted organisations that collect data for reasons that they felt were not necessary were challenged and the group felt less comfortable with this. They want to be involved in deciding what is acceptable to them.
4. **Who does the data benefit?** Where there was a clear benefit to the user the level of comfort was higher than where the benefit lay with a profit-making organisation.



1. **Police using facial recognition to look for a suspect on CCTV.**
   Not seen as problematic as largely it felt this was a justified use of CCTV.

2. **Police using CCTV and facial recognition to monitor public places.**
   Other examples which may be less clearly defined for police use felt more uncomfortable if there was ongoing monitoring. The question seemed to be about proportionality and transparency, how would people know if it was happening or not.

3. **Facial recognition to enter a gym, instead of a swipe card.**
   Gym access control – less comfortable than police use (the group appeared to trust the police more than a private business). The group were quick to say there were plenty of adequate alternatives that don't require biometric data, which suggests concern over secondary purposes 'what else would a private business use this for.'

4. **Shopping centre security guards using CCTV and facial recognition to recognise banned people coming into a shopping centre.**

   Similar result to the police cases – clarity of the use-case is important, and people are making comparisons to other safety arguments (i.e. CCTV?). Questions raised included: How long does footage like this need to be kept for people to feel safe, would it be used to create profiles? How reliable (accurate?) is it? Some comments about level of discomfort with being under 'constant surveillance.'

5. **Shopping centre using facial recognition to analyse how people move around the shopping centre to improve the layout of the shopping centre.**

   There was a feeling that people were less comfortable with this as it was felt to be more for the centre's benefit than theirs. People were more willing to participate if the example contributed to their safety, rather than just a private interest. *We didn't explore the potential for this to be done without identifying people.* There was an immediate concern around the necessity of something like this, but this may have moderated if we explained how this case may differ from some of the others re: potential identifiability/re-identifiability.

6. **Shopping centre detecting faces and characteristics to display targeted adverts on digital billboard content, for example advertising toys to children or sports kit to people who run past.**

   This was seen as much more closely aligned to an advertiser's private interest (profit) and for that reason people felt less comfortable about it.

7. **Facial recognition used in school canteens for payment, instead of a swipe card.**

People did feel that they were more comfortable with the school doing things like this than the gym example, which was a private company operating in a more 'public space.' In a school scenario it was felt that the school was more accountable and had more responsibilities to the welfare of the pupils than a private firm would. This meant that the data collection here felt 'more personal' as they already had a relationship with the school.

8. **Facial recognition in schools to make sure only students and teachers come in instead of swipe cards or access codes.**

Was seen as convenient and again, they trust the school. If it makes you safer, this is something they would probably be supportive of.

9. **Facial recognition in schools to mark attendance, instead of swipe cards or a register.**

This was not seen as necessary, or as a safety issue – it was seen as a school discipline issue which is at least one order of magnitude lower than pupil safety. This means that overall, this use case was challenged as not necessary. Delegates stated very clearly that they wanted a say in deciding what was considered necessary, and to have an active role in the decision – (this is a big push for student engagement in DPIAs and consultation/planning of new use cases to strengthen school's evidence that the proposal is necessary and proportionate. Schools as PAs couldn't rely on legitimate interests as this activity would be considered part of their core stat functions.

10. **Emotion recognition to analyse student behaviour and attention levels in class.**

Very uncomfortable with this use-case. Was associated with a lack of freedom, an infringement of their rights and generally considered intrusive. The concern was to be 'labelled' as not paying attention which the group felt was not very inclusive or fair way to support individual students. There was also a concern that something like this could fundamentally change the relationship between a teacher and pupil if the assessment of a pupil were reduced to the measurement of specific data points. This was then turned round by the group who considered emotional recognition in a classroom during lesson time as an aid to teacher training. Where the focus/product of this was the teacher (not them) they were much more comfortable with the proposal.

11. **Analysing the way customers type and hold their phone to reduce online banking fraud.**

Online security was seen as very important (a repeat of the safety narrative seen earlier). Identity theft/fraud can have serious consequences, and even some short-term issues and inconvenience. There was a question about the accuracy of this measure in isolation, and a view was taken that in order for the reliability of this to be acceptable, it should be one of a number of measures, in order to protect people from the risk of false positives.

12. **Emotion recognition to analyse gamer behaviour to adjust the level of difficulty in virtual reality or augmented reality games.**

This could be beneficial, but it was considered that there were other ways to do this. Others were more comfortable with this and thought that the objective here (a more fun game) was in the best interests of everyone. It was also seen as less concerning as it was assumed this was something you had direct control over whether

you participated or not. Also, there was a question about consent here and the motivation of the company collecting the data.

13. **Age verification based on face analysis, to make sure adults don't use services designed for children.**
Few comments here. People saw it as another safety use-case which made sense. After some initial lack of clarity on the specifics of the use-case, a delegate suggested this may be online safety from grooming. The overall responses probably reflect the view of this specific example.

14. **Age verification based on face analysis, to make sure people under a certain age don't access inappropriate content (eg checking someone is over 13 before signing up to social media)**
Broadly comfortable with this as it increases safety. There was one reference to the potential risk of other adults (older siblings/family) overriding this feature.

15. **Automatically comparing a selfie to an ID document to check someone up for a service is who they say they are.**
The group were generally comfortable with this, and some had encountered this before.

16. **To access a device like a laptop or phone, instead of using a pin code**
Generally accepted use case that the group were familiar with and felt comfortable using.

Thoughts on a 'Golden standard' for biometrics

At the end of the day young people were given a gold card and two statements to consider - one relating to organisations responsibility to educate young people and one relating to their responsibility to protect young people.

If they were writing this guidance, what would they want it to say?

In summary when it comes to education young people would like:

- Clear information that is easily accessible to young people about how their information is being collected, used and who has access to it.
- Clear education in schools about their data rights and biometrics, this could include seminars, written publications, presentations or visits from external organisations.
- Organisations to undertake surveys so they know the level of understanding of their users and can educate accordingly.

And when it comes to protection young people would like:

- Greater protection for children when biometric data is being collected.
- Consent to be clear, able to refuse easily and clarity of when consent will be needed from a parent or guardian rather than a young person themselves.
- Access to their data to be limited with no (or very limited) third party access.
- Purpose of data collection to be transparent and to only to be used for the original, clearly stated purpose.
- Ability to withdraw their data or a time limited period for data to be stored.
- Provide a clear outline about how the use / storage of biometrics data could impact a young person.
- Be approved as a suitable collector of biometric data by a regulator.

In order to EDUCATE young people organisations should…

- They should give out notices or a pamphlet guiding them on how and where their information will be going or being used for.
- Debrief young people about where their data is going and who has access to it. Also I think there should be an option to withdraw.
- Make easily accessible information that young people will read e.g. not small print or text designed to be difficult to read.
- Encourage schools to teach information on the topic.
- Prioritise the copious amount of vital information concerning the place and record in which their biometric (whether that be physiological, physical and or behavioural) will be stored and analysed. As a child, this information is inherently overwhelming and stress-inducing. Seminars which break down such consequences and actions that may be done by themselves should be mandatory and integrated into the curriculum in order to develop our approach towards such a topic that can easily have so many negative, intrusive connotations.
- Have included in curriculum.
- Make it more accessible and child friendly book.
- More school visits from official government organisations.
- Easy access to engaging and digestible info
- Info about pros and cons of using biometrics to the company.
- Info about pros and cons of using biometrics to the young people.
- What will the biometrics be replacing / improving?
- Offer guidance about how young people can protect the sharing of their biometric data (to prevent 'spoofing')
- Have biometrics included in the curriculum?
- Let the company's guideline be displayed on the company's website.
- Learn their right's (shown on the ICO website)
- Do school presentations and also try to implement some form of guidance to the younger generations especially since they are more present online.
- Clearly explain what biometric technology they are using, how they are using it and why to create a transparent experience.
- Explain how their data is used.
- Tell them their data rights and how they can take control of their data.
- Ensure that all possible shareable data is public.
- Conduct regular surveys into the understanding of their user base.
- Volunteer to share information of their own volition.

- Allow users to opt in and out of certain biometric data types.

In order to PROTECT young people organisations should…

- In order to protect young people organisations should tell parents or have age limits on when they are allowed to take a child's biometric information
- Keep data safe and stored with limited access (not everyone can access it) Furthermore organisations should ensure biometrics are used for appropriate things.
- Recognise that young people of a certain age are not responsible to give consent and their parent/guardian should do instead.
- Not take advantage of young people's vulnerability
- Present a range of options as to how children's biometric data should be stored, and the intricate methods used to analyse as such.
- A coherent understanding of the way in which biometric data is analysed and to visualise this. Having a grasp of the process provides great comfort and increases the chance of submitting the data. Withdrawal of submitting biometric data at whatever age when matured would only aid in our approach to biometric data as they feel as if it is being cautious with our data.
- Educate children more.
- Make it clearer what they are consenting to.
- Make sure to limit third party access to certain data.
- Be transparent.
- Put safety as top priority.
- Disclosing information more clearly and digestible
- Set a baseline of how data is collected e.g. can't be sold to a third party.
- It's about spreading awareness.
- Provide a clear outline about how the use / storage of biometrics data could impact a young person.
- Have a clear understanding of data protection laws.
- Keep information only for intended use.
- Be clear about how the data will be shared, where and for how long
- Give young people the opportunity to refuse or withdraw consent.
- Be able to withdraw consent at any time.
- Children under 16 not able to consent for themselves.

- Data collected not used in the future e.g. low attention in the classroom from data now means that it is difficult to get hired in the future.
- Implement biometrics / tech so that children that are more vulnerable / lack of awareness about these organisations such as FACE ID - to protect these children.
- Limit use of biometrics to effective use cases
- Have a clear use case and use for the data.
- Strict security and protection for the data
- Ask for parental consent to obtain the data.
- Be stored in a secure location.
- Only be used for a defined / specific purpose.
- Ensure under 18's have their consent approved by a guardian.
- Not store data long term
- Be approved as a suitable collector of biometric data by a regulator.
- Ensure that users are aware of any third parties that data will be shared with
- Allow users access to their data upon request.
- Organisations should always be transparent with the people using their biometrics and outline all their rights and options.

Feedback on the Workshop

Participant Feedback

Overall the participant feedback was incredibly positive with lots of young people commenting how much they enjoyed the workshop. One young person particularly enjoyed the case studies and would have liked to have done more of these as they were informative and prompted good conversations.

One participant shared how their confidence had grown by being involved in groups such as this and their gratitude for their involvement.

"I just wanted to let you know how rewarding today was for me- I learnt so much and met some amazing people! Thanks so much for putting it all together. I'd be really keen to participate in similar events in the future!"

" I really enjoyed the day and got a lot out of it. Thank you for having me."

Facilitator Reflections

Overall the day provided rich data for the ICO, and the group were engaged throughout.

One facilitator reflected that:

"Might have been worth explaining to the group the difference between 'raw' biometric data/images and the biometric templates which are derived from them? A whistlestop tour of how some of the use-cases work? Might have been challenging with limited time and an assumed mixed level of comfort from the audience."

The British Youth Council would like to thank the ICO for commissioning them to deliver this work and hope to work with them again in the future.