Consultation Workshop: Scottish Biometrics Commissioner

June 2025

Overview

What was the purpose of the workshop?

The Scottish Biometrics Commissioner wanted to hear directly from young people as part of the development of their next strategy. The workshop also explored the principles of the Code of Practice and the dissemination of the strategy to young people.

Method

What did the workshop involve?

- Meetings and follow up work to plan the workshop with Members of the Scottish Youth Parliament. The MSYPs were involved in planning and facilitating to ensure the workshop was youth-led, engaging and met the needs of the young people and the buyer.

- The delivery of a 1.5hr online workshop with a group of MSYPs to discuss and share views on the agreed topic through a series of youth-work activities.

- This report summarising the discussions following the workshop.

What was the process of developing the workshop?

SYP staff worked with one MSYP – Jack – to develop plans for the workshop in consultation with the Scottish Biometrics Commissioner staff. Jack is the Convener of SYP's Justice Committee.

The SYP staff met first with Diego Quiroz from the Scottish Biometrics Commissioner to discuss a general overview of the workshop, the aims and intended outcomes and gather information for the partnering MSYPs to feedback on. Jack provided feedback on:

- The session plan
- The accessibility of the session's presentation
- How overall youth-friendly the session appeared to be

The draft session plan was shared with Diego in advance of the workshop with opportunity for comments and edits. A copy of the full session plan is enclosed in this summary report.

On the day, workshop participants (a total of 11 MSYPs aged 16 – 22) were asked to:

- Consider how children's rights are reflected in the principles in the Code of Practice
- Consider potential future issues the Commissioner's office should focus on during the next strategy
- Consider how the Commissioner's office could communicate the forthcoming strategy with young people

They engaged in these discussions by using online tools, including Mentimeter and Canva Whiteboard. SYP staff then analysed the notes and survey data using a thematic analysis for qualitative data.

Findings

Activity 1: Children's Rights and Biometrics

Participants were given a brief overview of the key articles of the UN Convention on the Rights of the Child, including right to express their views freely and have their views heard in decisions that affect them (Article 12), the right to privacy (Article 16), the right to an identity (Article 8) and the right to be treated with dignity and respect if you are accused or guilty of breaking the law (Article 40). The facilitator then spoke over the guiding principles in the Biometrics Code of Practice (using the Easy Read descriptions developed by the Commissioner's office).

Respect for human rights of individuals and group: A participant felt this principle was inadequate in relation to the Equality Act 2010. There was a concern around algorithmic bias when processing biometrics. It was felt to be a necessary principle but to be effective, it needs to go beyond the code of practice with concrete actions.

Equality and wellbeing: A participant questioned whether this principle was actively promoting equality and the right to privacy (as detailed in UNCRC Article 16), and whether minoritised groups are protected in the same way.

Privacy and technology: A participant felt 'privacy' and 'technology' felt oppositional and questioned whether they can be grouped or presented in a different way to demonstrate the links and tensions.

AI: Participants had many questions about AI, including whether the organisations within scope of the Commissioner use AI; where is data being stored; whether AI use is being encouraged; and whether AI is being outsourced. Young people felt the language on AI needed to be strengthened.

Complaints: A participant asked about future plans to interlink services with complaints. There was a sense that there was lots of detail about what the SBC does not support but a lack of signposting to places that might provide support, such as the Information Commissioner and National Crime Agency.

Activity 2: Future Issues

Participants split into two groups for the next session, exploring potential future issues using 'what if' prompts. The prompts covered a broader scope than the current remit of the Commissioner to ensure young people could broaden their thinking on the issue. The 'what if' prompts are included in the annex for information.

The common themes included:

- **Young people's agency**

Young people raised the issue of control, both in relation to who can access their data and how it is used. It was felt if there were to be examples of biometrics being used to dictate or limit someone's choices, that was not positive. They felt that if biometrics were used to pre-decide a choice, this did not address the root cause of challenges, such as choosing healthy food. Notably, young people did not agree with this even when they assumed AI could use biometrics to make healthier decisions.

- **Transparency**

Some young people were relaxed about who had access to their data and how it was used, with the caveat that there was transparency and a choice to opt out if desired. Other young people felt transparency was a crucial issue to understanding why an organisation or company would need your data. Questions around transparency were also linked to personal safety. There was consensus within the group that biometric data should not be used for profit and if biometric data was collected that it had to be for a good and meaningful reason.

- **'Biopower'**

Young people were concerned about the potential bias and inequality in the collection and usage of biometric data, in particular from the standpoint of ethnicity. In addition, young people raised concerns about young people with additional support needs and their capacity for informed consent. Again, these conversations linked to safety with transparency and clarity allowing young people to be more confident (and thus safe) in how their data was being used.

- **Accountability**

Young people felt there needed to be tougher regulation on private companies using and accessing biometric data, including consequences for incidents of mishandling or when things go wrong. Young people recognised there might be serious personal consequences if data is misused or was inaccurate, and thus there needed to be mechanisms to make things right from the perspective of the data holder.

- **Cost Effectiveness**

Young people perceived biometrics to be expensive and complicated to roll out, and so even when they could identify benefits to using it, they generally thought that resources could be better used. For example, using biometrics within education settings could have a positive impact on preventing bullying but young people felt the resources would be better spent on improving school meals, buildings and more educational resources. This was also the case when different forms of biometrics were discussed, for example taking DNA samples versus fingerprints. Young people favoured cheaper, cost-effective methods of collecting biometrics.

Activity 3: Communicating the strategic plan with young people

The final activity was creative, using Canva Whiteboard to think about how the Commissioner can communicate the new strategy with young people. This activity was also carried out in breakout groups. Young people were given four prompts to shape their thoughts:

- What? Key messages
- Where? Key platforms
- How? Type of content
- Other thoughts

Key messages:

- Give young people the choice about their own data
- Young people understanding what biometrics are and what data you have
- Real life examples
- What are biometrics used for and who to go to if it is being used incorrectly. How can you protect your and your friends' data and privacy?
- Where to complain – not just the Biometrics Commissioner but also inter-service collaboration
- What are our rights?

Key platforms:

- Social media was the most popular way to improve engagement with young people with videos and simple infographics on platforms such as TikTok, Instagram, X, and LinkedIn.
- Young people thought posters in public places could be effective, such as libraries, active life places, youth hubs and groups, public transport (e.g. buses and trains), parks, home-educating forums, sports clubs.
- School and college were key places both for passive information sharing (like posters) and links with curriculum and learning (for example learning about biometrics in PSE classes or assemblies).

Type of content:

- Case studies – what are violations? What was the complaint? What was the result?
- Examples of ethical uses
- Integrated into larger data privacy conversations with links to other institutions
- Stats or information on how this is a fast-growing field and how important data can be in monitoring people
- Games that explain or teach and young people interact with

Other thoughts:

- A specific person who uses British Sign Language (BSL) would be appropriate for BSL-using pupils to learn about.
- Youth-friendly language and accessible with subtitles/large print/BSL
- Easy Read versions should include people as serious participants (rather than infantilising them) by using accessible text, flow charts, and images where relevant.
- Make it catchy!
- Should be young people in the videos – makes it easier to understand and relate
- Young people thought there could be a group of young people who could advise and create this content.
- Young people thought there was a possibility of the Commissioner having ambassadors or volunteers like Police Scotland Youth Volunteers (PSYV)

Further Information

If you require further information about the content of this report, please contact Emily Beever, Head of Policy and Public Affairs at emily.b@syp.org.uk.

Annex A. ‘What if’ prompts

- What if an algorithm chose what you could buy at the supermarket based on your DNA?
- What if the private company who owns and runs the fingerprint scanning system sells the data to another company without your permission?
- What if facial recognition was used to identify a bully in school?
- What if you needed to use facial recognition to enter school every day?
- What if your DNA was taken when you were born and was stored by the Government and police for your whole life?
- What if during online exams your webcam and microphone were used to monitor your movements and facial expressions to assess if you were cheating?