Leanda Barrington-Leach

INTRO

Thank you.

I am very grateful to be here today to discuss AI and children's rights.

I am Leanda from 5Rights, an NGO with the mission to build the digital world children and young people deserve.

As an organisation we work closely with kids, we do research, we work with IT practitioners on technical standards, and we provide expert support to regulators around the world.

I would like in the time I have been allotted now to set out 4 principles to help frame our discussion.

But first a few words on the issues.

Children online and regression of rights

Childhood today, is lived online as it is offline. The digital world is NOT optional for children.

Yet online children are not recognised.

Online everyone is equal, in other words everyone is treated as adult.

This has meant a massive REGRESSION in terms of children’s rights over the last 3 decades, as children’s lives are increasingly lived online.

Issues, risks

There is extensive evidence of significant risks to children’s physical and mental health and safety due to common AI systems, integrated into a wide variety of products and services that children use, from video sharing (70% of videos watched are the direct result of an AI recommendation) to gaming to search engines and chatbots.
The attention economy intentionally uses persuasive design to get and keep users online, engaging, sharing and creating content. This leads to children, particularly vulnerable to these psychological techniques, being systematically exposed to a wide variety of risks. Carelessly designed systems then exacerbate these risks and develop negative feedback loops for children and society as a whole.

Let me give you a few examples.

- 5Rights’ Pathways research showed that social media accounts registered as children were all subject to messaging from strangers and illegal or harmful content within hours of being set up. While these accounts were targeted with ads for games, sweets, teenage tampons and such like specifically for kids, they were at the same time also recommended harmful content, from sexualised to pro-suicide material, by algorithms that weight negative or extreme content 5 times higher than neutral or positive content.

- What does this lead to?
    - Consider addiction: 4-in-10 children say they rarely disconnect from social media and various studies find between a third and half of kids worry that they are addicted to the internet.
    - Consider commercial exploitation: Many online games are deliberately designed to extract as much money from players as possible. Essential aspects of the game such as energy and experience appear as resources that deplete before the player's eyes, with the option to pay to improve game play. 80% of apps marketed as suitable for 5 years olds contain in-app purchases. 15% of kids have stolen money to pay for loot boxes. Multi-billion dollar platforms such as TikTok and Roblox depend on children for free content creation.
    - Consider body image: 80% of girls have considered changing their appearance online and many will not post without a filter.
    - Consider gender stereotypes and violence: 10% of 10 year olds say they are addicted to porn. 80% of girls say it is common to be put under pressure to provide sexual images of themselves.
    - Or let's consider child sexual abuse. More and more child sexual abuse material is self-generated by kids, driven by groomers exploiting features such as friend recommendations, livestream, direct messaging and popularity metrics. The fastest growing category of CSAM is self-generated and involving 7-10 year olds.

- And just to be clear about the vicious circles we are creating: 70% of people who view child sexual abuse online first viewed the material when they were under 18. 40% first saw it when they were under 13. 51% say the first time they saw CSAM was accidental; they stumbled across it through a pop-up or as a result of a recommendation system. Similar vicious circles drive gender-based violence.

4 principles

How can we make sure the digital world is one where children can thrive?

First, we must recognise childhood online. That children have specific rights until they turn 18 will seem obvious to everyone in this room but is not commonly recognised among digital policy-makers, let alone tech companies. Online, what protections there are for children generally apply only up to the age of 13. This is because of a piece of US marketing law called COPA, and has been reinforced by the EU's GDPR setting the age of consent for data processing between 13 and 16. Consenting to the processing of data in order to access a service is NOT the same thing as giving up your rights as a child!

A child of 13 is not an adult, and in many ways older children are at greater risk – since younger children access fewer products and services, have greater adult supervision and spend less time online. All children deserve protection.

Second principle: Children have existing and established rights, which apply online as they do offline. We do not need to reinvent the wheel or await specific new research and analysis to apply these rights in the digital environment.

UNCRC General comment No. 25 sets out very clearly how children's rights apply online. Some of its provisions, regarding for example the protection from content, contact, conduct and contract risks, and the requirement of businesses to undertake child rights impact assessments, are reflected in the CoE Strategy.

I would like to cite one more:

- That data protection, privacy-by-design, safety-by-design and other regulatory measures ensure that businesses do not target children using techniques designed to prioritise commercial interests over those of the child.

Picking up on that. Third. Safety by design. The digital world is almost entirely privately owned, and human built. It is a system that can be engineered and optimised for any purpose. So, optimising for growth is a choice. Optimising for ad revenue is a choice. Optimising for engagement is a choice. Optimising for children's safety – or as we currently have it – failing to optimise for children's safety is a choice also. Safety by design, starting with a risk assessment and then a mitigation strategy – or purposefully designing for wellbeing and child users – should be an industry norm. Undoubtedly there are some sacrifices needed - from shareholders or from time to time from frictionless convenience for some adult users – but for the most part it requires the sector to do what it does best – provide a personalised user journey – in this case with the understanding that the user is a child. Child centred design is rarely a question of innovation or technology; it is almost always question of corporate and political will.

Fourth. We should not ask children, parents or teachers to hold the responsibility for badly designed systems. In our work with children, we have often observed that those children that have done e-safety courses have a tendency – when something goes wrong – to blame themselves. Why? Because most digital resilience is geared to bad actors and bad behaviour but fails to explain how the system promotes bad outcomes for kids. The sector is responsible for 25% of world GDP but still there is an idea that young children should be resilient to persuasive design or responsible for navigating its harmful content. And if not kids themselves we talk about educating parents and teachers, and asking them to use parental controls and continuously spy on their children. For absolute clarity – of course children, parents and teachers should be digitally literate – but that is not instead of creating a digital world that has already been designed with children's rights in mind.

Implementation

Practically, how can we implement these principles?

In every single piece of digital legislation we still need to fight for recognition of the basic principles that:

- A child is anyone under the age of 18.

- Children’s rights apply wherever children are in practice, as in across ALL platforms and services that they use or that impact them, big or small, and whether or not they are designed specifically for children.
- Children have a right to access; we should not just shut them out.
- The best interests of the child should be prioritised above commercial interests, and children have the right to an environment which is safe, private and secure, by design and default.

A system for CR in the digital environment requires:

1. Legal minimum standards for age-appropriate design
2. Age assurance, which must be privacy preserving
3. Child impact assessments and risk mitigation for all products and services likely to be accessed by children
4. Radical transparency and rigorous regulatory oversight

It is critical that the CoE’s legal instrument on AI reflects these principles and elements, and I count on many of you in the room today to ensure this message is heard and taken into account.

-/-

In conclusion, AI already plays a central role in children’s lives and there are massive opportunities to harness it as a force for good for education, for play, for free expression and exchange. For this to be true it needs to be designed with children's rights, interests and well-being front and centre. Until we have a system in which safety of children comes before optimisation for profit and growth we will not have the digital world children deserve.

Thank you.