

Online Safety Conference Keynote Address

Date: 23 November 2021
10.30am – 1.00pm

Keynote Speaker

Leanda Barrington-Leach is Head of EU Affairs at [5Rights Foundation](#). Leanda joined 5Rights from the European External Action Service where she was Adviser to the Secretary General focusing on Strategic Communications and the fight against Disinformation. She previously worked in EU advocacy as a consultant and for non-profits, always with a focus on human rights. Leanda volunteers as an Adviser to Plan International, supporting their work on children's rights in EU foreign policy.

@LeandaBL

@5RightsFound

Keynote Address

Thank you – I am LBL, Head of EU Affairs at 5Rights, a children's rights NGO with the mission to build the digital world children and young people deserve.

I am grateful for the invitation to speak today at this critical time for children's rights in Ireland, in the UK where our organisation is headquartered, in the EU where my work is focused, and globally.

I would like in the time I have been allotted to set out 5 principles that might help frame the conversation you are about to have with the most important speakers of the morning on the 'youth panel', and to keep in mind as you consider the provisions of the Online Safety and Media Regulation Bill. I will then finish by looking at where these principles have been used in a practical way, and the challenges and opportunities that remain.

But first a short reminder of the issues that have brought us here today.

Childhood today, is lived online as it is offline. Pretty much all kids are online, and they make up a substantial chunk of users of digital services – 1 in 5 in the EU. These kids - our own children, those of our friends, our professional charges, children we don't know in the street or playground – whoever they are and wherever they are, offline we keep an eye on them, we ensure they live, play and learn in environments that are as safe and conducive to their well-being and development as we

can. We certainly treat them differently from adults, because we recognise that as children they have specific vulnerabilities and needs.

But this is not the case online, where these kids spend A LOT of their time.

Online what we take for granted in the physical world is the exception rather than the rule.

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

The digital world is not optional for children, and yet it is a place where children's rights have been systematically overlooked, ignored, undermined - dare I say trampled.

Some examples:

Children are routinely served up harmful content - and not in small doses. Pornography, violence, pro-suicide, pro-anorexia... The impact is real and can be horrific. I recently learned for example that 70% of consumers of child sexual abuse material were first exposed to this content before the age of 18 - 40% of them when they were under 13. More than half of them were not looking for this material. Just take a moment to think about that vicious circle – and it works similarly for hate speech and radicalisation, misogyny, eating disorders and other such topics which I think our young friends will tell you more about later – think about this and the society that we are allowing these systems to create.

Children are also routinely introduced and contacted by adult strangers via friend and follower recommendation systems. Accounts of children as young as 11 have been recommended to groomers on popular social media platforms.

Children are routinely nudged to lower their privacy settings, spend more time online and engage in age-inappropriate behaviour. Note for example that 80% of the top 50 games rated suitable for children 5 and under in the Apple App Store contain in-game purchases.

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

First, we must recognise childhood online. A child is a child until they mature not only until they pick up a smart phone. Which sounds, as we say in the UK, 'bleeding obvious' until you recall that for the most part the current age of adulthood in the digital world is set at 13 – because of a piece of US marketing law known as COPPA. 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. The UN Convention on the Rights of the Child sets out clearly the requirements of a safe and secure childhood. As we develop a digital world fit for children and childhood we should not be reaching for new or lesser rights, but rather deliver on the well thought out privileges and rights they already have claim to.

Over several years, 5Rights served as consultants to the UN Committee for the drafting and consultation – with experts, member states and children – of General comment No. 25 which sets

out in detail how children's existing rights apply in the digital environment. The General comment prescribes among others, and I cite:

- That in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child must be a primary consideration.
- That children must be protected from content, contact, conduct and contract risks.
- That businesses undertake child rights due diligence, in particular child rights impact assessments.
- 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, from shareholders or from time to time the 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 to hold the responsibility for badly designed systems. In our work with children, we have often observed that those children that have recently or repeatedly done e-safety classes and courses have a tendency – when something goes wrong – to blame themselves. Why? Because most digital resilience and digital literacy is geared to bad actors and bad behaviour but fails to explain the nudges and focus of the system on growth, sharing and engagement 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 or responsible for navigating its pollution. For absolute clarity – of course children should be digitally and data literate – but that is not instead of creating a digital world that has already been designed with them in mind.

And finally, digital equity and empowerment. Safety is not a separate component to either of these things. Without dealing with ubiquitous porn, misogyny, religious and race hate, misinformation and scams, moderation in minority languages, oversight of data sets and algorithmic bias etc - then children both here and in the global south will be denied meaningful access and or will be disempowered when online. A lack of safety holds back progress for all – but importantly– it is particularly regressive for girls and for children of colour – or minority religious groups. Child online safety is an essential part of equity and empowerment – including the opportunity to have a stake in building and innovating our collective future.

So, practically, how can we implement these principles?

Firstly, that we need to LAY DOWN THE NORM, and specify in our digital legislation 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.
- Children have a right to high levels of protection, by design and default.
- The best interests of the child should be prioritised.

Secondly, we need to SET MINIMUM STANDARDS.

Even when companies and designers want to ensure the rights of kids, time and again we hear: "oh, I never thought of that!".

It is the job of the regulator to ensure that designers, companies, know what to think of and the standards against which they will be judged.

Here, a lot of good work has already been done or is in the works.

Firstly, regarding children's data protection. In the UK 5Rights Chair Beban Kidron introduced into law the Age Appropriate Design Code. This Code is based on the understanding that the features and practices designed to gather data are often intrusive or risky for children – so data protection has the ability to protect children by dialling down those features.

It is important to note that while the Code was much resisted when first suggested - this summer we saw a radical redesign focused on children's safety from all the platforms as they sought to meet the 2nd September deadline for compliance.

I don't have time to go into the changes, but they ranged from preventing direct messaging between children and adults they don't know, high privacy settings by default, turning off auto play, disabling notifications after 9pm, safe search for under 18's – as well as widespread changes to targeted advertising, data collection and sharing and the introduction of new wellbeing measures. What is more important than any single change is that the code put children's safety at the top of the 'to do' pile for the first time.

We are delighted that the Irish Data Protection Commission has taken a similar approach with its Fundamentals for a Child Oriented Approach to Data Processing. We see the Code inspiring initiatives to set standards for children's data protection from Sweden to Australia, the Netherlands to the US and Canada, and we hope to see the European Data Protection Board soon begin work on common Guidelines – perhaps with Ireland in the lead.

The second main avenue for change is by setting the norm and standards for all online services, as your Online Safety and Media Regulation Bill aims to do.

My colleagues in London are currently heavily engaged in the equivalent UK bill, which has a strong mandate to protect children. The expectation upon which the Bill is built is that companies will have to duty to consider the impact of the products and services on children. Just like the Age Appropriate Design Code, its premise is that you should be providing a safe and secure environment for your customer – particularly when that user is a child. The Bill focuses on the systems and processes of services, like their algorithmic recommendation systems and design features that create the scale and reach of harm, rather than on specific types of content. It is underpinned by risk assessment requirements, and in this respect takes a safety by design approach.

At the EU level we are also working on the Digital Services Act, which has the potential to require service providers to systematically assess risk and undertake mitigating measures, with strong transparency and auditing provisions.

There is also the AI Act, which proposes to ban outright AI systems that exploit the vulnerabilities of children.

EU Product Safety Regulation is equally being updated to bring all digital products – i.e. anything that can be downloaded onto a physical device – into scope of stringent consumer protection legislation. This is great because it is based on the precautionary principle: if you can't prove your product is safe, you can't put it on the market.

Finally, we are expecting a proposal soon on preventing and combatting child sexual abuse online, which will hopefully include strong provisions on safety by design.

-/-

Let me finish with a word about parents. You would not expect a parent, doing the school run, to check the air bag, the steering wheel alignment, the speedometer, to check that the break pads are working or that the road signs have not been removed– for those things you rely on manufacturing standards and the department of transport. A parent's job is to check the wing mirror before they pull out. This is what we need to do with the digital world. This is not a problem solved by parents and children but rather a question of product safety and sufficient regulatory oversight – because 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.

Notes:

You can watch a recording of the #123OnlineSafety Conference [here](#)

For more information about the #123OnlineSafety campaign visit, [1 2 3 Online Safety Campaign | Children's Rights Alliance \(childrensrights.ie\)](#)

Or contact Emma Archbold, Campaign Lead: emma.archbold@childrensrights.ie