

UN High-level Panel on Digital Cooperation: Response of the 5Rights Foundation

January 2019

The 5Rights Foundation works towards a digital environment that anticipates the presence, meets the needs and respects the rights of children. Our interdisciplinary network includes: child development experts, online protection experts, lawyers, technologists, NGOs, campaigners, academics, policy-makers, and many from the commercial sector.

The 5Rights Foundation is currently working on behalf of the Committee on the Rights of the Child to create a General Comment on Convention in relation to the Digital Environment. The General Comment will clarify how this rapidly evolving environment impacts on the full range of children's rights in positive and negative ways. Its purpose will be to strengthen the case for greater action and elaborate what action is required by States in order to meet their obligations to promote and protect the rights of the child in and through the digital environment.

We welcome the commitment of the UN High-level Panel on Digital Cooperation to take a leadership role in this important area – a role it is well-placed to fulfil - and appreciate the opportunity to contribute.

Below we set out the values and principles that we believe should underpin cooperation on addressing issues with the digital environment, including our seven pillars for an Internet Safety Strategy. We have provided examples of where cooperation has been successful to date, both in the digital environment and offline, and we make a series of recommendations for action. Our submission is concerned particularly with the need for digital cooperation to consider the needs of children, including but not limited to autonomy, privacy, safety and that their views are heard.

For further evidence or information, please contact Jay Harman at jay@5rightsfoundation.com.

Values and Principles

Recognise the Concept of Childhood

The digital environment was conceived as one in which all users were equal, and it continues to operate in this way. In fact, 1/3 of the global population are under 18 – children.

In practice, this means that the privileges, protections, and rights that collectively constitute the concept of and legal framework for 'childhood' do not meaningfully exist in the digital environment. The failure to recognise the concept of childhood has resulted in the widespread treatment of children as if they were adults. In a UN context, the needs and

rights of childhood are codified by the UNCRC. If the routine failure to recognise childhood online continues, the Convention will increasingly offer children little or no protection.

5Rights supports the creative and *intentional* use of digital technology by children and recognises that access to it is essential to their wellbeing and flourishing in the modern world. However, it is clear that digital access must go hand in hand with providing an environment in which children's needs are met and their rights are upheld in order that they may flourish, free from fear, free from undue risk, and free from commercial exploitation.

Our principal recommendation is therefore that:

Childhood must be recognised in the digital environment, because *in an interconnected world* the failure to uphold the privileges, protection and rights of children in the digital environment will erode childhood itself.

Global and Consistent Standards

Above all, cooperation on addressing digital issues must be underpinned by a desire to see global, consistent, and enforceable standards implemented around the world. Given the transnational nature of the technology sector and the issues it throws up, cooperation must focus on finding solutions that apply across borders. This is not to say that solutions cannot be instigated by a nation state or region and then be successfully adopted globally.

The EU's experience to date with the General Data Protection Regulation (GDPR) and its precursors has demonstrated the ability to drive better practice among digital service providers and to assist with the enforcement of regulation. The 5Rights Foundation is also currently developing *Universal Standards for Childhood*, working with standards agencies around the world, including the Institute of Electrical and Electronics Engineers (IEEE) and British Standards Institute (BSI). These will create effective guidance, impact assessments, technical standards and certification models for those manufacturing, operating and delivering services in a digital environment. The standards seek to create a world fit for children and childhood, and are being developed for global use and adoption.

It is worth noting that this global approach is already common in a range of other sectors. Aviation regulation, for instance, is harmonised around the world to ensure consistent levels of safety, overseen by the UN's International Civil Aviation Organisation and its national equivalents.¹

The alternative – a patchwork of internationally inconsistent regulation - has caused and continues to cause problems. For instance, the report on content regulation published by the UN Special Rapporteur on Freedom of Opinion and Expression last year detailed the way in which some states have demanded and sought to require extraterritorial removal of links, websites and other content alleged to violate only their local law. 'The logic of these demands', according to the report, 'would allow censorship across borders, to the benefit of

¹ See 'about us', The International Civil Aviation Organization (ICAO): <https://www.icao.int/about-icao/Pages/default.aspx>

the most restrictive states¹, potentially jeopardising the free expression of individuals irrespective of the legal protections in their home state.² The Child Dignity Alliance's Technical Working Group report on preventing Child Sexual Abuse Material (CSAM) similarly outlines the way in which variations in the classification of CSAM across borders hampers detection and take down.³

Definitional inconsistency can be just as problematic as regulatory inconsistency. The *Luxembourg Guidelines* that seek to establish common definitions relating to the protection of child sexual exploitation and abuse were developed explicitly in response to concerns that confusion over terminology may hinder effective prevention and elimination of child sexual exploitation.⁴

We recommend that international stakeholders develop formal mechanisms to share evidence on the impact and effectiveness of legislative and non-legislative measures, including standards, relating to the digital environment, as well as mechanisms for the swift adoption of best practice.

Stakeholders should also work towards the adoption of universally shared definitions in describing the digital environment and the issues that arise within/from it.

Inclusion

As a general and guiding principle, cooperation on addressing the issues brought about by digital technology must include engaging with and considering all those who are affected by those issues. Given that one third of the global population are children, it is particularly important that their experiences, needs, and views are heard and acted upon.

In doing so, children must not be treated as one monolithic group. If the solutions to issues created by the digital environment are to be relevant to all children, then the diversity of different ages, developmental stages, locations, and vulnerabilities that exists within that group ought to be reflected. We refer the Panel to 5Rights' report *Digital Childhood*, which proposes, among other things, that childhood development milestones are used to inform policy and practice in addressing digital issues.⁵ It should be emphasised, too, that children tend to be over-associated with issues of safety and under-represented in discussions about

² Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (content regulation), April 2018 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

³ Child Dignity Alliance, Technology Working Group Report, 2018: <https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf>

⁴ Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, 2016: <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>

⁵ Baroness Beeban Kidron (5Rights) and Dr. Angharad Rudkin (University of Southampton), Digital Childhood: addressing childhood development milestones in the digital environment, 2017: <https://d1qmdf3vop2l07.cloudfront.net/eggplant-cherry.cloudvent.net/compressed/01972a9579924cbba7943c849bf159b3.pdf>

algorithmic fairness, democracy, veracity of information and news etc. Engaging properly with children and young people will ensure that this does not continue to be the case.

In considering the circumstances of individual children, stakeholders must also consider the needs of distinct groups of children who may require particular and special consideration. For instance, the digital environment has been proven hostile to girls, particularly in their teens,⁶ and children with special education needs or disabilities and children cared for by the state, among others, have been shown to face particular challenges online.⁷

Additionally, it is essential to consider the many millions of children who do not yet have access to the digital environment. Cooperation should of course work towards delivering access to those who do not have it, but access for children must never come without first ensuring their established needs and rights.

A Note on Innovation

All those cooperating on solutions to digital issues must be resilient to claims that regulations, standards, or any other forms of obligation placed upon the technology sector stifle innovation. Online safety and innovation are not mutually exclusive. Rather, introducing standards to which all companies must adhere can serve to level the playing field by allowing new players to enter the market with prior knowledge of its rules. In any case, where there is genuine conflict between innovation and online safety, it is the role of international institutions, governments and regulators to find in favour of the best interests of the child.

Seven Pillars

In January 2019, 5Rights published *Towards an Internet Safety Strategy*, which set out ‘seven pillars’ on which any safety strategy should be built.⁸ The model we set out is universally applicable and the values it encompasses could and should underpin efforts to address digital issues all over the world. It respects and acknowledges the benefits of digital technologies, while seeking to transform the relationship between children and the technology they use.

The seven pillars are:

- **Parity of protection**
- **Design standards**
- **Accountability**
- **Enforcement**

⁶ Girls’ Attitude Survey 2018, Girlguiding, 2018: <https://www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2018.pdf>

⁷ Vulnerable young people and their experience of online risks, Adrienne Katz (Youthworks) and Dr Aiman El Asam (University of Kingston), 2018: <https://www.saferinternet.org.uk/132-vulnerable-young-people-and-their-experience-online-risks>

⁸ 5Rights Foundation, *Towards an Internet Safety Strategy*, 2019: <https://d1qmdf3vop2l07.cloudfront.net/eggplant-cherry.cloudvent.net/compressed/4f41b5307f0dc41d3a7d6e44f8712221.pdf>

- Leadership
- Education
- Evidence-based interventions

First Pillar: Parity of Protection

The norms and expectations of society that apply offline must apply in the digital environment too. To differentiate the two is to misunderstand the way in which technology impacts on both society and the lives of individuals. We do not live on and offline – our reality is organised, interrupted, augmented, and sometimes dominated by technology. In order to deliver on any societal contract, standards, expectations, laws, and rights must apply seamlessly and equally both on and offline.

We recommend that Nation States undertake to make clear in their own domestic legislation and regulatory contexts that rules apply equally on and offline. In particular, individual Nation States should bring forward legislation that formally transposes the responsibilities of companies, organisations, and individuals vis a vis children from the offline world to the digital environment.

In the UK there is growing support behind proposals to introduce to the digital environment a concept already well-established in the ‘physical world’: namely a ‘duty of care’.⁹ In sum, a duty of care would require digital service providers to take reasonable steps to prevent foreseeable harm from arising to their users. Such a duty would inherently drive a precautionary approach¹⁰ that in turn would result in better safety by design (see below). This would encourage a design culture that would make the experience of the digital environment more in line with expectations that have already established in the physical world.

We recommend a Duty of Care is implemented not just in the UK but around the world, with a view to driving better safety by design across all digital services and ensuring that the protection of all digital users, regardless of their location, are considered in advance. Such a duty would specifically articulate the additional protections offered to children under the age of 18.

Second Pillar: Design Standards

It is necessary for services to be designed in a way that is transparent, fair and safe – by default. Responding to digital harms and negative social impacts after the event, as has historically been and is currently the case, is ineffective. The much more effective approach is one that seeks to address digital issues at the design stage before they have arisen.

⁹ Professor Lorna Woods and William Perrin, Reducing Harm in Social Media Through a Duty of Care, 2018: <http://blogs.lse.ac.uk/mediapolicyproject/2018/05/10/reducing-harm-in-social-media-through-a-duty-of-care/>

¹⁰ The Precautionary Principle: Protecting Public Health, the Environment and the Future of Our Children, 2004: http://www.euro.who.int/_data/assets/pdf_file/0003/91173/E83079.pdf

This approach is already embedded in and across all other sectors, from road safety standards¹¹, to building regulations¹² and food safety requirements.¹³ An effective example of it in the digital environment is the Content Accessibility Standards¹⁴ that have transformed the online experience of those with disabilities. The *Age Appropriate Design Code* (the Code) currently being introduced in the UK to require service providers to deliver the highest level of data protection for children and young people by design and default is another.¹⁵ In fact, we would recommend that:

The Age Appropriate Design Code being introduced in the UK should be used as a model for similar statutory regulation around the world. The UN High-level Panel on Digital Cooperation should engage with the Information Commissioner's Office in the UK with a view to sharing internationally its experience of formulating and implementing the Code.

It is important to stress that 'better by design and by default' is an approach that must apply to systems as much as it does to content. This is the approach that the Age Appropriate Design Code takes. Content standards are clearly important in mitigating the content risks faced by children online, but standards governing aspects of system design like device security, privacy settings, user-engagement features or features that drive certain behaviour are equally important – if not more so – in mitigating the contact, conduct, and contract risks to which children are also exposed.

Third Pillar: Accountability

To date, the digital world has not been characterised by either transparency or accountability, and the technology sector has not owned – or been required to own – the impact of the services it provides. This must change. The technology sector must be responsible for the impact of its services, just like all other sectors, and governments around the world must require it to do so. In this sense, accountability cannot simply be a *value* underpinning cooperative efforts to address digital issues, it must be formed in agreements and legislation as an *obligation*.

In practice, this might mean introducing a range of provisions like 'health warnings' or research access to certain categories of commercial data, but at the very least it requires:

A 'regulatory backstop' to ensure enforcement of a company's own rules and community guidelines. Companies are free to set their own rules, but since they are so poorly upheld, we must introduce a mechanism to ensure that published terms are upheld. *Routine failure* to deliver on a company's or organisation's own published terms must be subject to an enforcement regime. We note that in the UK a significant majority of children under 13 have

¹¹ ISO Road traffic safety management systems

¹² Building Regulations 2010

¹³ Food Standards Agency Guidance

¹⁴ HM Government, Web Content Accessibility Guidelines (WCAG 2.0), 2017: <https://www.w3.org/WAI/standards-guidelines/wcag/>

¹⁵ Information Commissioner's Office, Age Appropriate Design Code, 2018: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-age-appropriate-design-code/>

a social media account in spite of the minimum joining age being 13 in most cases.¹⁶ This is a failure of the published rules of companies at such a scale as to demonstrate clearly that the self-regulatory approach has failed – and that a regulatory backstop is required.

Mandatory transparency reporting against predetermined measures. Meaningful transparency cannot be achieved while companies determine what types of information, in what level of detail, they will or won't share. Reporting standards ought to be set out by a regulator (with power to demand information if necessary), which should also set expectations for responses and outcomes in relation to any shortfalls. Again, this would be more powerful if done commonly across jurisdictions, but in any event should be done by willing governments on an individual basis.

Fourth Pillar: Enforcement

Cooperation between private companies and governments and service users cannot continue to be premised on the idea that regulation is only necessary where technology companies fail to respond to particular incidents that make it into the public consciousness, and that ought to have been prevented in the first place. Rather, both private companies and governments must accept that the fast pace of technological development demands an enforceable regulatory regime irrespective of how capable the sector claims to be at dealing with its issues at any given time. This allows for clarity of expectation and consistency of user experience.

'Enforceable' is the key word here. A regulatory regime needs to be properly resourced and it must have powers of enforcement and sanction that meaningfully bite on large, trans-national corporations. In this sense, enforcement is not so much a principle underpinning cooperation but a necessary precursor to it, ensuring that the technology sector engages with other stakeholders even where they might otherwise be disinclined to.

The GDPR is an example of how properly enforced regulation can spread good practice internationally, and indeed impact on service design around the world too. The enforcement of the GDPR, and indeed its predecessor the Data Protection Directive, through European courts has also demonstrated that regulation that starts in a single area can be made relevant globally to even the very largest transnational corporations.¹⁷

There is no reason why the introduction of equivalent regulation for other issues that emerge from digital services could not produce similar results.

Fifth Pillar: Leadership

Leadership in the traditional sense of the word is obviously needed to drive both cooperation and action. The EU is already acting as a global leader in delivering a robust

¹⁶ According to Ofcom's Children and Parents Media Use and Attitudes 2017 report, 51% of UK 12-year-olds, 46% of 11-year-olds, and 28% of 10-year-olds now have social media profiles:

<https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-parents-2017>

¹⁷ E.g. *Google Spain SL v Agencia Espanola de Proteccion de Datos* (The Right to be Forgotten)

international response to online safety, and we welcome the UN's commitment to doing the same.

Effective leadership also means clarifying which state or supranational actors have responsibility for different aspects of a regulatory regime. Clearly allocated responsibility not only aids cooperation between regulators around the world, it also facilitates compliance by making clear to whom the technology sector is accountable. The UN could usefully provide a skeleton framework for adoption and enhancement by nation states that offers a map of regulatory functions and institutions.

Sixth Pillar: Education

Education is a key component of any safety strategy. There are two mistakes that need to be guarded against, however.

First, education is frequently used to demand that users, particularly children, be resilient to a system that does not respect or protect their safety and security. A safety strategy should never lose sight of the fact that its primary goal is achieving system design that is safe by default. Second, education can be compromised by the insistence that technology companies should be responsible for delivering it. There is currently concern about Google's suite of educational programmes deployed widely in UK and US schools, which somewhat uncritically present 'Google as impartial and trustworthy'¹⁸ while failing to provide information about risks associated with the 'sector norm', such as profiling, compulsion, and the impacts of data collection.

Education clearly ought to include all of these things, but it must not focus simply on safety. A broader focus on digital literacy and skills is both the best way of keeping children safe and the best way of ensuring they are prepared to flourish in the digital environment.

Finally, an effective education programme should not be confined to schools and school-age children. **Tertiary education** must introduce ethics and safety by design modules to computer science and related disciplines. **Professional training** and continual professional development for anyone who works with children – teachers, social workers, health and legal professionals – ought to include online safety. **Parents**, too, should be given accurate and consistent guidance on internet safety from trusted sources.

Seventh Pillar: Evidence-based Interventions

There is a growing body of evidence on harms,¹⁹ and while there is a need for further longitudinal research in some areas, that should not stand in the way of immediate action to protect users or promote children's wellbeing (see for example *The precautionary principle*:

¹⁸ 'Google is teaching children how to act online. Is it the best role model?' New York Times, 23 October 2018: <https://www.nytimes.com/2018/10/23/business/google-kids-online-safety.html>

¹⁹ S. Livingstone et al, Children's Online Activities, Risks and Safety: a literature review by the UKCCIS Evidence Group, 2017: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf

protecting public health, the environment and the future of our children, World Health Organization, 2004).

If cooperation and action are to be evidence-based, there first needs to be a commitment from all stakeholders to gather evidence free of commercial interests and funding. Commercial actors should make privately held data sets available for research, and government should have powers to require this where it is in the public interest to do so. The wealth of expertise and knowledge in academia, policy, government, and the private sphere – not to mention the user-base – must not be siloed off from one another, and if necessary more formal information-sharing infrastructures should be introduced. Perhaps above all, the sharing of evidence and ‘what works’ in tackling digital issues must be shared between countries, so that interventions can be consistent wherever possible.

Finally, in the case of children there is a tendency to ask questions in language that they may not fully understand or in terms that they do not relate to. Children’s views are also frequently sought but then not responded to or acted upon, which deters them from engaging as fully and honestly as they might. In Scotland, the Young Scot 5Rights Youth Leadership Group are an exemplar of good youth engagement. After spending several years advocating for children’s views to be heard, the group now act as official advisors to the Scottish Government, providing evidence and insight from young people based on a deep critical understanding of the issues and sector and their own experience of the digital world.

Summary of recommendations

Childhood must be recognised in digital settings. It is the responsibility of both the technology sector and governments around the world to ensure that this happens.

Relevant legislation and regulation in individual nation states must apply equally on and offline. In particular, individual nation states should bring forward legislation that formally transposes the responsibilities of companies, organisations, and individuals vis a vis children from the offline world to the digital environment.

Global, consistent, and enforceable standards should be implemented internationally. Given the transnational nature of the technology sector and the issues it throws up, cooperation must focus on finding solutions that apply across borders. This is not to say that solutions cannot be instigated by a nation state or region and then successfully adopted globally.

Formal mechanisms for sharing evidence and best practice must be introduced to facilitate global adoption. Mechanisms should be developed to share evidence on the impact and effectiveness of legislative and non-legislative measures relating to the digital environment, as well as mechanisms for the swift adoption of best practice.

Universally shared definitions should be developed and adopted in describing the digital environment and the issues that arise within/from it.

The Age Appropriate Design Code currently being introduced in the UK should be used as a model for similar statutory regulation around the world.

The ‘duty of care’ approach to regulating digital services should be introduced around the world, with a view to driving better safety by design across all digital services and ensuring that all digital users, regardless of their location, are properly protected.

A ‘regulatory backstop’ to ensure companies’ adherence to their own rules and community guidelines should be implemented globally. Companies should continue to be free to set their own rules, but *routine failure* to deliver on them will result in sanction or enforcement action.

Companies must complete mandatory transparency reporting against predetermined measures. Globally consistent reporting standards ought to be set out by an international regulatory body and enforced locally by state-specific regulators, with powers to set expectations for responses and outcomes in relation to any shortfalls.

Conclusion

In the above we identify children and young people as forgotten, even invisible, stakeholders in the digital environment, despite making up 1/3 of the population globally. We set out how their needs can be met, their rights upheld, and their voice heard by challenging the status quo of weak accountability and service design.

We have also set out the principles that we believe should underpin cooperation on the digital environment - chiefly a commitment to implementing universally applicable and enforceable standards, guided by the involvement of the children and young people those standards seek to protect. The values and principles that different stakeholders should seek to embed in the solutions they develop are encapsulated in our Seven Pillars.

As the examples above demonstrate, cooperation can be and has been successful, both in relation to the digital environment and the offline world. We believe that with a commitment to learn from these examples, to share knowledge across sectors and borders, and to harmonise the best interests of users with the commercial interests of the technology sector, the digital environment can become one in which all people, children included, are able to flourish.