Explanatory Notes

General comment no. 25 (2021) on children's rights in relation to the digital environment

5RIGHTS FOUNDATION

The purpose of these explanatory notes is to offer further understanding and provide tangible, real-world examples which illuminate the provisions of general comment no. 25, produced by the UN Committee on the Rights of the Child.

The digital environment covers a vast range of intersecting circumstances and contexts and it is not possible to capture all of them. These notes are intended to anticipate questions and signpost to approaches that have been brought to our attention and reflect the particular concerns that were raised in the course of research and drafting.

The text is drawn from contributions made to the UN Committee on the Rights of the Child by expert groups, children, members of the 5Rights steering group and the 142 submissions to the consultation and workshops with 709 children in 28 countries. While these Explanatory Notes and the contributions that fed into them do not have the authority of the general comment itself, they provide more contextual insight, and we remain grateful to every contributor for their invaluable input.

Many submissions referenced the significance of Covid-19. While the pandemic accelerated some children's adoption and use of digital technologies and extended their interactions and time spent online, children's reliance on the digital world predated and will continue long after the effects of the pandemic. Covid-19 increased children's reliance on multiple digital technologies to exercise their basic rights to education, information, and participation. However, the pandemic also threw a spotlight on a digital divide which exists between the digital "haves" and the digital "have nots", both within countries and between them. The pandemic has exacerbated and therefore widened pre-existing educational inequalities, and these remain a concern both for the short and longer term. One question was repeatedly put forward, how much longer will it be before access to digital technologies will be considered a fundamental right for every child?

As digital technologies impact on children's lives in ever increasing ways, it is vital to consider the *full spectrum of children's rights* against the *full range of the impacts* of digital technology, both now and into the future. General comment no. 25 does just that.

The numbering of the Explanatory Notes mirrors the paragraphs of general comment no. 25. It does not replace the general comment and is limited to explanations and examples that relate to the general comment text. We hope over the months ahead that others will help add to add to the best practice examples and we ask readers, particularly those colleagues in the Global South, to support us in the effort of making this a richer and more representative document.

5Rights Steering Group
March 2021

Explanatory Notes

I. Introduction

1. Over 1000 children were consulted during the drafting of this general comment. They have contributed to In Our Own Words, a children's version of the comment, and a summary of their views can be found in Our Rights in a Digital World. Their views have been taken into account by the UN Committee on the Rights of the Child and are reflected in general comment no. 25.

2. Definitions of the listed technologies can be found in the glossary (Appendix 1). Many people consider the digital environment to be what happens on a computer or smart phone and in a rather obvious way it is. But the digital environment is a continuously and rapidly evolving and complex environment which involves many interconnected technologies, some of which may be in a child's hands while others are not directly possessed by them but still impact on their lives. Children's rights will in the future be impacted by technologies that do not currently exist.

   Moreover, even if an individual child is not a user of a particular digital technology, their rights may be impacted by virtue of it being used by others. The list provided in Appendix 1 illustrates the breadth of the digital technologies that make up the digital environment, but it is not comprehensive. Children's rights are relevant in respect of all actions and impacts of the digital environment, whether listed or not, and to all current or future digital technologies.[1] Given the pace of technological change and evolution, and the challenges that accompany such changes, it is highly likely that 'new' future technologies will continue to impact children's rights in a multitude of ways. In that sense this general comment should be viewed as a guide to the interpretation of the Convention on the Rights of the Child to be used on a continuing journey, rather than being a travelogue for the here and now.

3. Children who live in connected societies are finding that technology mediates and impacts most areas of their lives. Increasingly, governments may use AI to allocate resources or services, or distribute and provide access to them. For example, in South Africa, relief grants for families impacted by Covid-19 can only be applied for electronically.[2] Remote learning platforms may be used for teaching, or perhaps, a 'smart' ID card or biometric system may be used to identify a child on public transport or to allow them to enter a building. Children are also using many products and services that connect them to family, friends and others. These products are often designed for adults and have commercial purposes including data processing and features that may adversely impact a child's experience or violate their rights.

[1] For resources on the evolving nature of the digital environment, see for example, https://www.cigionline.org/
[2] https://www.gov.za/covid-19/individuals-and-households/social-grants-coronavirus-covid-19

Equally, technological systems can be used to spread knowledge or distribute services to children in ways that benefit them and enhance or strengthen their rights. Technologically-mediated services can bring genuine opportunities to improve inclusion and to overcome inequality or disadvantage. But even here the systems may be only partially understood by their users and can therefore introduce both unknown, and known, risks. For example, in Australia the use of AI to detect welfare fraud proved inaccurate and caused many families to have their payments revoked.[3] The ways in which similar AI systems process information and make decisions is often opaque to the very people impacted by these technologies. AI is also commonly used in recruiting[4]: making automated judgements of applicants' suitability for a job or educational opportunity, or life altering decisions made in the justice system. It is not always the case that children, or their parents, are aware of the impact of automated technologies. As a consequence, many children feel anxious about whether the digital world can be trusted.

4. Having meaningful, safe access to digital technologies can support a child to flourish.[5] Digital technologies allow children to connect with each other to peruse their interests, can help them access services and environments that contribute to their development, and is an environment in which they can participate in civic and cultural life. For example, as referenced earlier, at the first peak of the pandemic in 2020, 1.6 billion school children around the world could not attend school.[6] While children with access to the digital world were able to participate in remote learning, for many children who had no access or compromised access (sharing devices, limited data), learning opportunities were curtailed. Access inequalities (or a lack of equitable digital inclusion) contribute to already existing educational inequalities.[7]

   Access alone is not sufficient. Children must have safe, trusted means to use technologies in ways which enable them to realise their rights, while mitigating the risks that accompany such access.

> **"Currently we are not using any of the digital technology to express ourselves but would like to if we have knowledge or access to it in the future"**
>
> Ethiopia, age and gender unknown[8]

5. General comment no. 25 does not emerge from a vacuum. There has already been a significant contribution to the examination of the intersection of technology and human rights. This general comment draws on that expertise and experience, including foundational UN documents such as the UN Guiding Principles on

[3] https://www.theguardian.com/technology/2019/oct/16/automated-messages-welfare-australia-system
[4] https://www.bbc.co.uk/news/business-55932977
[5] https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_ACCESS.pdf
[6] https://www.weforum.org/agenda/2020/12/covid19-education-innovation-outcomes
[7] https://unctad.org/system/files/official-document/dtlinf2020d1_en.pdf
[8] Our Rights in a Digital World, p. 10

Business and Human Rights[9], and strengthens it further through wide-ranging consultations to examine the particular implications for the human rights of children in relation to business,[10] and by drawing on other UN documents. Particular note should be made of the consultation with children.[11]

6. General comment no. 25 refers to other general comments and Optional Protocols to the Convention on the Rights of the Child that provide additional detail on particular subject matters,[12] notably:

- General comment no. 2: The Role of Independent National Human Rights Institutions in the Protection and Promotion of the Rights of the Child
- General comment no. 5 (2003): General Measures of Implementation of the Convention on the Rights of the Child
- General comment no. 7 (2005): Implementing child rights in early childhood
- General comment no. 9 (2006): The rights of children with disabilities
- General comment no. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)
- General comment no. 16 (2013) on State obligations regarding the impact of the business sector on children's rights
- General comment no. 17 (2013) on the right of the child to rest, leisure, play, recreational activities, cultural life and the arts (art. 31)
- General comment no. 19 (2016) on public budgeting for the realization of children's rights (art. 4)
- General comment no. 20 (2016) on the implementation of the rights of the child during adolescence
- General comment no. 21 (2017) on children in street situations
- General comment no. 24 (2019) on children's rights in the child justice system
- Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2019)[13]

[9] HR/PUB/11/04 https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
[10] http://childrenandbusiness.org/
[11] Children's Consultation report
[12] Accessed here: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=5&DocTypeID=11
[13] https://www.ohchr.org/Documents/HRBodies/CRC/CRC.C.156_OPSC%20Guidelines.pdf

II. Objective

7. General comment no. 25 sets out how children's rights apply in the digital environment. It will help states to understand what steps are necessary to respect protect and fulfil children's rights in all environments including the digital environment.

III. General principles

8. The four following rights in the Convention have been identified in the Convention on the Rights of the Child as general principles that must be taken into account in the implementation of all other rights and in respect of all aspects of children's interactions with digital services and products.

A. Non-discrimination

9. Increasingly, children need to have access to digital technology in order to develop and flourish. States need to undertake specific programmes to ensure equitable access, including for children who might not have broadband or devices at home. For example, Project Isizwe provides dedicated WiFi hotspots at Curro schools in South Africa.[14] Children also need the skills to use the technology provided.

   States must include, within National Action or Development Plans, a roadmap for addressing and bridging any digital inequalities, especially for girls, children from poorer communities, children in rural and/or remote areas, and children who lack relevant content online, particularly in languages other than English. Where possible, states should impose universal access obligations, and ensure children have access to affordable or free data plans so they can complete educational assignments and participate. Where children are unlikely to have private and personal access to digital devices and the digital environment, governments should make provision for public access. However, public or shared access to digital devices and the digital environment will rarely be an appropriate longer-term alternative to private and individual access. While states vary in their capacity to provide digital access to the general public, the point is the children, and especially particular subgroups of children, should not be discriminated in the planning and delivery of such services.

10. Discrimination can take many forms. Some children are wholly excluded from participating in digital environments; for example, girls who face restrictions in their societies may also be restricted from accessing the digital environment.[15]

"Girls seem to have less access to internet than boys… There is a

[14] https://www.commscope.com/globalassets/digizuite/470-300-cs-project-isizwe.pdf
[15] https://plan-international.org/education/bridging-the-digital-divide

> **discrimination in access based on gender… Girls do not actually own their own phone and have limited access to the internet compared to boys, who might access it through the internet cafes that are generally only for boys."**
>
> Jordan, workshop facilitator's notes[16]

In some contexts, children have been forced out of digital environments through online abuse[17], or they can be discriminated against by virtue of the assumptions and decisions of larger digital systems which can lead to structural or indirect discrimination (for example, the use of an algorithm to grade exams in the UK in 2020, which disproportionally lowered the grades of students from lower-income areas against their teachers' predictions).[18]

11. Discrimination in all forms must be tackled, whether perpetrated by individual actors, an institution or as a result of the digital ecosystem itself. The committee calls on states to take proactive measures in policy and legislation to promote equal access to the internet and digital technologies for all children.

B. Best interests of the child

12. The 'best interests of the child' is a principle that must be applied to decisions that affect children in the digital environment. When there are competing interests between, for example, adults' rights to online freedom of expression and children's rights to privacy, states must ensure that the best interests of the child or children are a 'primary consideration'. For example, the UK Information Commissioner states in relation to children's data protection that "*it is unlikely however that the commercial interests of an organisation will outweigh a child's right to privacy*".[19] The principle can also be applied to help determine responses to situations where there are tensions between children's different rights, for example, the child's rights to freedom of association through online forums, against the child's right to protection from cyberbullying or exploitation. Wherever possible, the determination of what is in a child's best interests should also take full account of the child's own views.[20]

13. Children should be given a voice in determining the best interest of the child. The focus of policymakers and civil society is often exclusively on child protection in the digital environment, but children have a wide range of rights and all their rights including those to participation, freedom of information and freedom of thought

[16] Our Rights in a Digital World, p. 13
[17] Our Rights in a Digital World, p. 17
[18] https://www.technologyreview.com/2020/08/20/1007502/uk-exam-algorithm-cant-fix-broken-system/
[19] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/
[20] https://digitalfuturescommission.org.uk/blog/the-best-interests-of-children-in-the-digital-world/

must also be considered. Children must also be consulted and are often very clear about how they would like their digital world to embody their rights.

> **"Technology is very important, and it will continue to be in the future... The world is moving forward, and so we must do the same."**
>
> Croatia, girl, 12[21]

C. Right to life, survival and development

14. There are significant numbers of known and emerging risks to children facilitated or enhanced by digital technologies. States must take all measures to prevent risk and protect children from harm that may impact on their emotional development or physical survival. States should mandate routine risk assessment from service providers to identify risk under the four Cs (Content, Contact, Conduct and Contract[22]) and put all necessary measures in place to mitigate those risks. Many states have introduced legislative and regulatory regimes to deal with specific or groups of risks. For example, 150 countries have refined or implemented new anti-child sexual abuse material (CSAM) laws in the past 15 years[23], and the European Commission has produced a Code of Conduct on illegal online hate speech.[24]

15. Children need direct and ongoing interaction with their parents or caregivers and other family members, especially at an early age. Face to face and physical contact is vital for all aspects of their development. Use of online devices and screen based activities must not be a substitute from such contact. Training for parents and carers to understand child development and how digital technologies impact on development should be provided, rooted in reputable, evaluated research across all age groups such as the Digital Childhood Report[25], which considers the needs and autonomy of various age groups in their interaction with the digital environment.

D. Respect for the views of the child

16. Children are early and enthusiastic adopters of digital technologies. States should seek and take account of children's views about matters that affect them including on how to enhance the opportunities the digital environment affords, and how it can help them develop the skills and opportunities to participate in cultural and civic life.[26]

---

[21] Our Rights in a Digital World, p. 4
[22] https://www.riskyby.design/the-risks
[23] https://www.icmec.org/csam-model-legislation/
[24] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en
[25] https://5rightsfoundation.com/uploads/digital-childhood---final-report.pdf
[26] https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/10_cases_of_child_participation_report.pdf

> **"Digital technology plays a role because with [its] help... we can connect ourselves to the world and we can make an identity in the world."**
>
> Pakistan, boy, 13[27]

17. Legislators, businesses and organisations that create, deliver and govern the digital world should consult with children. Children often have strong views and creative ideas about how to maximise the benefits and minimise the harms of the digital world and can make a positive contribution to a rights-respecting digital environment.

> **"Every website should make it mandatory to start your account as private and you can decide to make what public whenever you want."**
>
> Young person, UK

18. Digital technology itself can be used to consult with children. For example, the children's version[28] of this general comment was developed through virtual workshops and an online survey with open questions. This allowed us to quickly and easily consult and reach 215 children from 28 countries.

    Consulting with children digitally must not result in violations of their privacy. Neither should they be punished for their views or obliged to reveal their thoughts. Children without access to digital technologies should not be excluded from participating in similar consultations: they also have views about how the digital world might help them realise their rights.[29]

    As a prior condition of meaningful engagement with children, it may be necessary to inform or educate children about digital technologies or their rights. [30]

[27] Our Rights in a Digital World, p. 7
[28] https://5rightsfoundation.com/In_Our_Own_Words_Young_Peoples_Version_Online.pdf
[29] https://www.coe.int/en/web/children/participation
[30] https://digitalfuturescommission.org.uk/wp-content/uploads/2020/10/Children-and-Young-Peoples-Voices.pdf

IV. Evolving capacities

19. Children's capacities and levels of understanding evolve throughout their childhood, and are influenced by their context, experience, expectations and opportunities. Children's active engagement with digital technologies can help them to develop their capacities in relation to a broad range of information, facilitating their learning, sharing of experience and participation in their community in ways that can reinforce and enable their growth and understanding. Being in contact with other people, including other children, supports their agency, self-worth and belonging, and spurs them on in their own development. Not all children or contexts are the same. The way they use and experience the digital environment will change according to their context and evolving capacities.

Researchers and policymakers are still debating the pros and cons of the impact of technology on child development. Many countries have established guidelines on children's technology use, though most of these focus on protection and more attention is needed to guidance on obtaining the benefits of access.[31]
Industry age restrictions can be poorly signposted, inconsistent or differently applied by different platforms. They may also be poorly upheld or driven by commercial considerations which bear little relation to children's level of development and understanding. These can result in wide-spread age-inappropriate content and contact being offered to children of all ages.

States should take all possible measures to ensure that children of different ages are encouraged not to engage with products and services that are inappropriate for their age. For potentially harmful content, age rating, systems which identify what age or age range a product or service may be suitable– for example, the Pan European Game Information (PEGI) system indicates the minimum age that a video game is deemed suitable for, based on content such as violence, sexual content, or bad language.[32] Such tools should not prevent children accessing content for the general public, nor unduly narrow the range and diversity of content they can access, nor prevent them from accessing particular content that they need to enjoy their civil rights and freedoms.

However, States should not concentrate solely on content – but consider the pressures and behaviours that services demand of children. Guides to these pressures including UNICEF's AI for children[33], and 5Rights Foundation's Risky by

[31] https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282019%293&docLanguage=En
[32] https://pegi.info/page/pegi-age-ratings
[33] https://www.unicef.org/globalinsight/featured-projects/ai-children

Design[34], suggest the use of child impact assessments as part of development of products and services as exemplified by the Australian E-Safety Commissioner.[35]

20. Products and services are often designed by adults for adults and do not take into account the needs of children. Digital practices for example services streaming, e-commerce, and social media often promote behaviours and worlds that are beyond the capacities of the child that is affected. For example, misinformation sources promoting far-right views on Facebook have an average of 65% more engagement per follower than other far-right pages, which is significant if children do not have the capacity to understand that something is false. [36] Children may require different protections at different times and by different service providers. It is not a given that older age groups require less protection, since many younger children are supervised, or older children may be accessing a broader range of products.

    States should take measures to make sure that the products, services and environments that children *actually* use[37] and those they are compelled to use have taken account of their needs. To uphold children's rights in digital environments, their rights and particular needs should be considered at every stage, from design to implementation, with relevant data protection and justice frameworks in place to uphold their rights in technological systems.

    Measures may be introduced by legislation, codes of conduct, regulatory action – but must be mandated and subject to public oversight, accountability and remedy. Children may think in sophisticated ways about, and offer valuable insights into, the positive and negative implications of digital technology. Children's participation in consultations, including discussions regarding the digital environment, should not be reduced to tokenistic one-off consultation processes or be confined to adult-defined issues for example the consultation process put forward by Council of Europe. These conversations must be ongoing. Decision-makers must ensure that, when the child is capable of forming his or her own views, these views are considered seriously. How children's views are considered and incorporated into decisions must be fed back to consultation participants.

21. Parents and caregivers have a unique role in children's lives and should be supported to understand the digital world. Support can be given through guides and country-specific services, for example, the ITU's global guidelines.[38] Children's evolving autonomy, capacities and need for privacy changes as they grow and develop. It is necessary to support parents and caregivers in acquiring digital literacy and awareness. This awareness should enable parents/carers to achieve an appropriate balance between protecting children and respecting children's

[34] https://www.riskyby.design/introduction
[35] https://www.esafety.gov.au/about-us/safety-by-design
[36] Far-right news sources on Facebook more engaging, Cybersecurity for Democracy, March 2021. https://medium.com/cybersecurity-for-democracy/far-right-news-sources-on-facebook-more-engaging-e04a01efae90
[37] Take the example of WhatsApp, which is restricted to users 16+ in Europe, but 14% of 12-15 year olds in the UK use it https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf
[38] https://www.itu-cop-guidelines.com/

emerging autonomy, for example, for young people exploring their sexuality; and young people seeking medical advice/treatment independently of their parents/carers.

While parents and carers need support, states should also require digital providers to offer or make available services to children that are appropriate for their evolving capacities including empowering adolescents to manage their own access to information, services and the personal and digital data that this generates. Recognising the different states have different national laws and age limits, states must still ensure that information and activities must respect all children's rights, including their right to privacy and to be protected from commercial exploitation and violence.

V. General measures of implementation by States parties

22. Legislative and formal structures will be needed and sometimes they will be needed ahead of formal evidence of risk or harm – for example, the Duty of Care proposed by the Carnegie UK Trust[39], aiming to prevent harm rather than respond after harm has been done.

A. Legislation

23. Many laws still refer to or envisage an analogue world and must be updated to specifically support enforcement and compliance in digital environments. States should review and update national legislation to ensure the digital environment is compatible with the rights in the Convention and its Optional Protocols. States should introduce and implement legislation to ensure that businesses respect children's rights and are held accountable if they fail to do so. States should also introduce laws and policies that prevent businesses from contributing to violations of children's rights and redress violations if they do occur. For example, businesses should undertake child rights due diligence processes.

In all legislation, there should be a focus on identifying risks and upholding children's rights before the onset of harm. To update and introduce legislation requires resources and must be made a political priority. In addition to legislative frameworks, states should invest in implementation by bolstering relevant regulators and law enforcement agencies, ensuring they have the necessary legal powers and technical understanding in order that they develop the capacity to uphold children's rights as entrenched in relevant legislation.

[39] https://www.carnegieuktrust.org.uk/blog/the-statutory-duty-of-care-and-fundamental-freedoms/

> **"I would change… laws [to ensure] companies don't have the power to use and share people's personal information without their permission."**
>
> New Zealand, girl, 16[40]

B. Comprehensive policy and strategy

24. Existing agreements about safeguarding children in specific circumstances, such as trafficking, commercial or consumer exploitation, health and safety legislation, etc. should be reviewed to ensure that they specifically refer to the digital environment. In some cases, governments may wish to develop a specific Child Online Protection policy, for example, as in Rwanda[41] and Ghana.[42] These should seek to enhance children's digital experience, not to prevent them accessing the digital environment.

25. In the balance of responsibility, it is important that businesses provide an environment that minimises risks for children. The physical world and the digital social worlds are closely intertwined, meaning that what happens 'online' is unlikely to stay there and what happened 'offline' is likely to find its way 'online'. Children sexually exploited 'offline' may be revictimized by the spreading of their image online. Images can be reproduced and reappear indefinitely on an enormous scale. Children who may have voluntarily produced sexualised images of themselves alone or with a partner, or children who have been groomed or coerced into sexual activity online can, after the fact be extorted or threatened with public disclosure in order to make them comply with further demands. It is imperative that all those who carry responsibilities for safeguarding children understand the impact of digital technology. Those who are responsible for the creation of digital technologies must understand the responsibility they have for safeguarding children against these risks.

    Policies should establish and promote training and guidance for children, parents and caregivers, relevant professionals and the public. These programmes should raise awareness of children's rights and how to protect them. In child-friendly formats there should be programmes targeted at children which aim specifically to develop children's digital skills and promote their awareness of the opportunities presented by digital technologies. Such measures should empower children to use the digital environment in a beneficial and safe manner. All victims and survivors should be aware of the remedies which are available to them if their rights have

[40] Our Rights in a Digital World, p. 26
[41] http://www.xinhuanet.com/english/2019-07/22/c_138248409.htm#:~:text=Having%20come%20into%20force%20in,Ministry%20of%20ICT%20and%20Innovation
[42] http://childsafety.gov.gh/

been violated and be given age-appropriate support to claim those rights or in certain circumstances obtain compensation for breach.

26. Children will access the digital environment in all the settings that they live in or visit. As a result, child online protection measures must be designed to protect children systemically – from the creation, uploading, spread or amplification of harm – whether they are, for example, at home, in alternative care, at school, in cybercafes. This means undertaking risk assessments when designing products and services, and disabling features where risks might outweigh the benefits for children, for example, direct messaging[43] or sharing real time locations with other users.[44]
While many children can play an important part in their own safeguarding, it is the responsibility of states and businesses that provide digital technologies to ensure that services or devices which they provide or promote are safe for children. Children's safety online must never be framed as a responsibility which falls primarily or exclusively on the child or their parent or carer. At the point of first use every service or device must be provided in a way which makes it as safe and as rights-preserving as possible for a child and all steps away from such a benchmark must be clearly labelled and the potential consequences explained.

C. Coordination

27. States should identify or establish a government body, institution or regulator mandated to monitor and coordinate policies and programs related to children's rights in the digital environment. States vary in whether they give the responsibility for such coordination to the Ministry of Family or Business or Education or Justice or some other body. The point is that the state's obligations regarding children's rights in relation to the digital environment requires multi-agency cooperation, and one institution must be tasked with coordination. This institution must be sufficiently resourced to cooperate with businesses, civil society and other organizations or stakeholders to realize children's rights and promote child safety in the digital environment. Such a body should be able to draw on technological, legal and other relevant expertise within and beyond government as needed – including from local and international child rights[45] and digital rights[46] NGOs and agencies, also its mandate should include collaborating with other governments and international organisations, to promote global interoperability and a high bar for digital policies. It should be funded in a transparent manner, with independent oversight over its operations (see paragraph 29.) This body should be independently evaluated for its effectiveness in meeting its obligations as well as its adherence to human rights standards. It should be clear to all stakeholders, including children and

[43] https://www.riskyby.design/the-risks
[44] https://www.theguardian.com/technology/2016/jul/10/pokemon-go-armed-robbers-dead-body
[45] For example, https://www.crcasia.org/
[46] For example, https://africadigitalrightshub.org/

parents/caregivers, which is the key coordinating body from which guidance can be sought and to which complaints can be directed.

D. Allocation of resources

28. In order to fulfil the obligation to ensure that children are able to exercise their rights fully, equitably and safely in the digital environment, States must make available the necessary resources. The digital environment is going to have a growing and ever more significant impact on the lives of children and States must invest sufficiently to ensure that every child is able to benefit without discrimination from this development.

29. While commercial companies should bear the costs of meeting safety and security needs of their 'child' customers, states must ensure that public institutions tasked with ensuring children's online safety have the resources necessary to implement appropriate policies and programmes to preserve and protect their rights in the digital environment, and the resources to monitor business compliance and investigate and where necessary prosecute and provide redress where they fall short. [47]

    These resources should be independent and not subject to direct or indirect forms of lobbying or other forms of pressure from political influence and business interests that may undermine the 'best interest' or other rights of children.

E. Data collection and research

30. The challenges of protecting and promoting child rights in a digital environment are changing fast and it is necessary to understand the emerging risks, user trends[48] and the impacts on children through up to date evidence - for example by use of the open-access research toolkit developed by Global Kids Online.[49] States should fund and capture, in a rights-respecting manner, comprehensive data and pay particular note of how digital technology impacts on different groups of children. Research can also be used to guide interventions and policy development that supports children's rights in the digital environment.[50] Research and public data collection must respect the full range of children's rights, including their privacy and rights to non-discrimination. Children themselves should be involved in the development of the research agenda as well as the research process itself. States should support the growing, but often unsuccessful, effort to obtain evidence from businesses about how their services are used by children, with what effect, and how children report/complain and in what numbers. Where appropriate, states should provide

[47] https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf
[48] For example, unsafe 'challenges' on social media services such as TikTok and Instagram may be amplified by recommendation algorithms, where these challenges can quickly spread and reach children. Two recent examples of such risky 'challenges' include the Blackout challenge which led to the death of a 10 year old girl in Italy, and the spread of a suicide video embedded in videos of kittens and puppies.
[49] www.globalkidsonline.net/tools
[50] https://www.unicef-irc.org/publications/1065-childrens-experiences-online-building-global-understanding-and-action.html

researchers with access to data that is anonymised about children's usage of digital technology to produce evidence that can guide policy.

F. Independent monitoring

31. Most national human rights institutions derive their mandate from legislation, and it is imperative that any mandate to investigate and address complaints clearly empowers them to also act in the context of the digital environment. However, given the reach and scale of the digital environment, coupled with the multi-factorial nature of human and children's rights, it is probably inevitable that multiple bodies will be involved in monitoring or enforcing children's rights. States should therefore ensure that there is proper co-ordination and full, public delineation of the roles and responsibilities of the different bodies involved.

G. Dissemination of information, awareness-raising and training

32. General comment no. 25 is specifically designed to set out states' actions and stakeholder responsibilities necessary to realise children's rights in the digital environment. To make these effective, it will be necessary for all parties to understand these obligations and duties. This requires broad public awareness including but not limited to children, parents, and caregivers, as well as specific training for policy makers, businesses and those who provide frontline services to children.

    Awareness programmes should also take account of children's lived experience and their views. Public awareness campaigns should cover the full gamut of risks (appendix) and should encourage the creation of a rights-respecting digital environment for children. Particularly, efforts should be made to ensure that such campaigns reach beyond the more privileged segments of society and encompass minority and disadvantaged groups. Parents and caregivers need information and skills to help them provide safe environments for children's digital engagement, but it should not devolve or delegate responsibility to children and their caregivers from governments or business.

33. Professionals working with and for children in all settings, including in education, health and mental health facilities, in social work, alternative care institutions, law enforcement, the justice system as a whole, and the business sector and those who design automated systems for these settings, should receive training that includes how the digital environment impacts the rights of the child in the multiple contexts, the ways in which children access and use technologies, and the impact automated systems may have on the future outcomes of a child. States should ensure that relevant pre-service and in-service training is provided.

    Those that develop digital technologies (including but not limited to the tech sector, public bodies and academia) should integrate training on children's rights into national capacity-building programs, pedagogical programmes, and design

standards. This is exemplified by Finland's National Child Strategy[51], which used the UN Convention on the Rights of the Child to consider how children's rights should inform every area of Finnish society. States should provide both initial and in-service training to ensure professionals remain up to date in the latest trends and knowledge.

These training efforts should cover principles of child-centred design, data protection, and children's rights, and need to recognise and take action against child sexual abuse. Design features that are known to be risky for children should be clearly identified, for example those that randomly introduce adults to children via friend suggestions. Positive features that enable children to exercise their rights should also be identified and encouraged, for example, online services for children that offer data privacy, so they can access support with no fear of contributing to their digital identity in a way they cannot control.

H. Cooperation with civil society

34. Many civil society organisations are active and knowledgeable about children's rights, and some specialist organisations have specific expertise about an area (or areas) of children's rights and/or digital experience. States should engage such organisations in the development of their policies and programs to ensure that they meet the best available standard for the promotion and protection of children's rights in relation to the digital environment. There is unlikely ever to be a truly "level playing field" as between groups or interests representing or advocating for children's rights but states have a responsibility to ensure such groups have the means necessary to perform their tasks to a satisfactory standard, and that their views, contributions and expertise are heard in relation to decision-making.

I. Children's rights and the business sector

35. General comment no. 25 is addressed to states, but the design and delivery of the digital world is largely in the hands of industry and other non-government organisations. For example, in relation to data protection, children seeking mental health services have found that their data were being sold to third parties[52] to target them with advertising, and non-white children have experienced being 'mis-identified' by facial recognition systems trained on white faces.[53] General comment no. 25 sets out the ways that businesses and other organisations should and can realise children's rights and what actions states should demand of business.

The effective evaluation of policy is often dependent on digital businesses themselves and the research which they fund or allow, e.g. by making data available to independent researchers. States should ensure that independent research aimed

[51] https://minedu.fi/en/strategy-for-children
[52] https://privacyinternational.org/node/3193
[53] https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

at providing well-informed, evidence-based contributions to further development of policy is enabled, for example by establishing large data sets as a public asset which can be accessed by organisations or universities engaged in appropriate forms of research.

36. States should fulfil their responsibilities by ensuring that companies are required to provide products and services that do not violate any children's rights in any environment. Steps must be taken to prevent violations and where violations may or have happened accessible, swift and effective routes to complaint and remedy should be the norm.

    Providing advice to parents and children is helpful, including advising how children can use products and services in ways that are beneficial to them, however advice is additional to, not instead of services that are designed to protect and anticipate children's presence and informal and formal routes for redress.

37. Individuals or coordinated groups may try to infringe children's rights in regular but incremental ways, for example health misinformation that results in a failure of children to be vaccinated[54] or in acute ways, for example by posting content that encourages suicide.[55] These problems can be amplified by the design and business practice of internet businesses, which tend to prioritise spread of information (reach), interaction with users, and maximising the amount of time spent online over moderation or creating age appropriate experience.

    States have a responsibility to protect children from infringement of their rights and both known and emerging risks, and where harm does occur, to act swiftly and robustly to adjudicate, redress and support children. States should ensure that business fulfils their responsibility to respect children's rights in a way that is consistent, transparent, accountable and enforceable.

38. States should require businesses to undertake child rights due diligence so that they identify, prevent, and mitigate their impact on children's rights including across their business relationships and within global operations. Given the heightened risks for children inherent in the digital environment, this should be a priority and should be closely monitored by the State. As far as possible reporting by businesses on the outcomes of this due diligence process should be made public and should be a source of learning and reflection to inform policy. States should undertake child rights impact assessments[56] of existing and new legislation to ensure the digital environment is compatible with the CRC and Optional Protocols.[57]

    States should not only take appropriate steps to "prevent, monitor, and investigate" violations of children's rights by businesses in the digital environment, but also take appropriate steps and draft appropriate legislation to take action when business

54 https://www.vox.com/recode/22319681/vaccine-misinformation-facebook-instagram-spreading
55 https://www.bbc.co.uk/news/av/uk-46966009
56 https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf
57 https://www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx

enterprises fail to adequately protect children from being violated within their digital environments.

39. In addition to national legislation and international treaties, it is necessary for all actors in the digital ecosystem to respect children's rights. Industry codes, design standards, terms of service and other activities that are undertaken in the development and deployment of digital products and services should be rights-respecting.

The possession of enormous data sets which can be used to test or develop new products or services is a key way in which established digital businesses can strengthen and extend their market dominance. This combined with the network effect helps create and sustain monopolies which may make business impervious to the call to respect children's rights.

States should encourage companies to develop digital products and services in the 'best interests of children' and ensure that the steps they have taken are transparent and in language understandable to children and parents/caregivers.

J. Commercial advertising and marketing

40. Many products and services are highly commercial and depend on processing user data to generate revenue. Designing to optimise for the maximum amount of data processing can have a profound effect on a child's interaction with their online environment, what they see, how their behaviour is altered, and how intrusive the service might be. Widely respected work has been done on this by Norwegian consumer bodies and NGOs.[58] Examples of the impact of such patterns can be seen when services offering progressively more extreme content, suggesting users add friends or speak to strangers, or using extensive notifications through the night and interrupting sleep can all alter the day to day lives of their users. Such products and services may not be considered rights-respecting, and should be 'toned down', 'switched off', or regulated in line with children's rights, for example rights to privacy, an inner life, or not being commercially exploited.

> **"Spending too much time on the internet causes people to not play, not socialize with parents and friends, and causes lack of sleep and mental illness."**
>
> Brazil, girl, 13[59]

Many of these features are not integral to the performance of the product and service that the child is using and are instead engineered to prioritise outcomes that

[58] https://www.consumerwatchdog.org/sites/default/files/2018-06/2018-06-25%20Deceived%20by%20design%20-%20Final.pdf
[59] Our Rights in a Digital World, p. 39

favour the private company. States should take steps to ensure that outcomes respect children's rights.

41. In the digital world, advertising takes many forms:

- contextual advertising: the seamless integration of advertisements into online content or digital services, allowing users to remain immersed in the content and services features whilst simultaneously being exposed to brand marketing and messaging;
- targeted advertising: the practice of showing particular adverts to users based on data collected about them, for example their online activity, purchases, location, gender, age, preferences, etc.;
- product placement: the inclusion of branded products in content not explicitly intended as an advertisement, with the intention of subtly promoting that product;
- influencers: social media users with large follower counts, who use their platform to promote their views and/or preferred products to their followers; and
- sponsored content: social media posts created by users under contract with brands to promote their products.

All children (as well as many adult users) have issues identifying paid-for content, which leaves them open to coercion. For example, the tobacco industry recently moved into using influencers to promote vaping.[60] Many influencers have very young audiences.

States should mandate that all commercial content is clearly labelled and identifiable and that advertising is always age appropriate. For example, the UK regulator has been working on an age-appropriate advertising framework.[61]

42. Policymakers should consider putting in place special protections for children such as a ban on using children's emotional data to market to them or their parents. For example, if a child expressed sad thoughts to her toy, it would be unethical, exploitative and a violation of privacy for businesses to advertise to the child's parent products to make their child happy.

Advertising in the digital world can be highly personalised. For example, in 2017 Facebook shared psychological insights on young people with their advertisers.[62] Even if platforms don't offer insight into children's mental states - children can be identified by having particular interests, for example, exercising and sport, which if

[60] https://www.reuters.com/article/us-instagram-vaping-idUSKBN1YN15B
[61] https://www.asa.org.uk/uploads/assets/uploaded/3af39c72-76e1-4a59-b2b47e81a034cd1d.pdf
[62] https://www.marketwatch.com/story/facebook-says-it-doesnt-target-vulnerable-teens-with-ads-but-it-has-studied-them-2017-05-01

identified leads business to make children targets for advertisements for health supplements, diet regimes or cosmetic surgery.

Information on any form of personal data processing should be given in a concise and clear way to parents or caregiver of the child. It is advisable to provide also an adapted version for children of the same information. Obtaining parental or caregiver consent does not exempt private institutions from following children's rights-by-design standards[63] or upholding children's best interests. States should have strict national laws that prevent using a child's personal data to target them with advertising.

K. Access to justice and remedies

43. Digital systems are often opaque and complex, and it is unreasonable to expect parents and children to manage violations if they have to act individually or expose specific children to scrutiny in order to get action from digital service providers. There is a disproportionate power differential between a child and global companies. It is often also unclear in what jurisdiction a case should be brought. Legislation should provide a clear framework to access to justice and remedy, such as the remedies, liabilities and penalties set out in the EU's General Data Protection Regulation.[64]

Many published terms (including but not limited to terms and conditions, community rules and privacy notices) are long, legalistic and unclear – the average child user or their parent or caregiver cannot understand them. Information should be given in a concise and clear manner, in formats that children enjoy, and that is easily understood by the child, or parent or caregiver. Providing information in accessible formats is not sufficient, the information presented should respect children's rights.

44. In order for children to have access to justice, they require robust legislation, access to expert help and provisions for collective action. And such action should be free, safe, confidential, responsive, timely and child-friendly.
It is important to note that knowledge of rights is separate and different from access to justice. States must provide mechanisms that hold business to account rather than leave individuals chasing global companies for justice.

Additionally, it is problematic that enforcement and regulatory communities are often not sufficiently trained to provide support for children in the digital world, with all its complexities, potential harms and jurisdictional complications. There is an urgent need to provide specialized training for law enforcement officials, lawyers, prosecutors and judges, to ensure that specialized services are designated to meet the particular needs of children, and that such services are adequately funded and equally accessible to children without discrimination.

[63] https://childrensdesignguide.org/
[64] https://gdpr-info.eu/chapter-8/

The data of children within the justice system is particularly sensitive and requires additional safeguards and protections. The records of children in contact with the criminal justice system should be kept strictly confidential and closed to third parties except for those directly involved in the investigation and adjudication of the case. Additionally, any form of remedy or procedure for addressing violations of children's rights and abuses of children in the digital environment must ensure that the confidentiality of a child victim's identity and other relevant personal information is protected.

States should ensure that children seeking justice are protected from retaliation or intimidation, whether by the alleged offenders, State actors, private sector actors, civil society, or family members. In bringing cases it can be that corporate structures are opaque, and there are questions of where and how claims can be brought. There is little existing case law and legal aid may not be available. States should ensure that privacy of victims is maintained during proceedings, legal aid is available and that routes to remedy include transnational cooperation. Business should be encouraged to provide effective grievance mechanisms of their own. Where appropriate, the State should also establish and resource a child-friendly mechanism for receiving anonymous requests to commence an inquiry based on pre-established and validated procedures.

45. Technical tools or products that identify victims and survivors or perpetrators must be complemented by strategies that offer routes to support for children. States must put support for victims and survivors into child protection frameworks and recognise that the spread of images pose a continual threat of re-victimisation. States should look beyond the most extreme crimes and ensure that redress and support is available for children for all sorts of rights abuses and that the nature and scale of the support is suitable for the violation. For example, the support and redress needed by children who have been targeted by scammers, or been discriminated against by wrongful inclusion on a database will be different from that needed by a child, for example, who has been coerced into joining a gang or who has suffered child sexual abuse.

There is much evidence that offender management programmes of re- education, for example, those assessed by EU Rehab Children[65], are an important factor in stopping the spread of abuse. These programs can be unpopular with politicians and public since they appear to be giving resources to perpetrators of heinous crimes, but experts make the point that a single perpetrator may have many victims and so each perpetrator taken out of the system is of benefit to many children. In addition, there is a need to understand how perpetrators operate. Such research is most valuable in order to refine prevention and protection programmes.

46. In addition to legal and governmental sponsored redress and reparation there are many cases in which the response may need to come from business. States will

[65] EU Rehab Children has published best practice guidelines from across Europe - http://www.famylias.org/wp-content/uploads/2015/05/Handbook-of-Best-Practices-in-Juvenile-Rehabilitation-Programs-in-Europe-LD.pdf

need to mandate standards for the design and deployment of digital technologies but also standards of moderation, response, redress and compensation. Company grievance mechanisms will have to take account of the age and development stage of children and should be transparent, independently accountable and enforceable.

States should provide opportunities for children and young people to appeal these remedies if disproportionate to the harm that they have incurred.

Specific attention should be given to developing a framework and effective resources to support children who themselves display harmful online behaviours. Responses to these behaviours should be educative, rather than punitive, recognising the social and contextual factors that may have contributed to the situation including the experience of making a complaint.

47. International co-operation is required for many violations, including but not limited to child sexual abuse, grooming by extremist organisations, scamming, fraud, stealing identities – and data violations. Barriers such as different definitions of categorisation of crimes, different standards of data protection, different protections for different age-groups – and a lack of understanding of either or both children's rights or the operation of digital technology – can prevent effective cooperation.

States should seek to share knowledge, bring definitions together and, should work to fulfil the demands of international initiatives for example the UN Secretary-General's High-level Panel on Digital Cooperation[66], the European Union's Digital for Development (D4D) Hub[67] and their first regional collaboration with the African Union.

48. States should ensure that national laws and regulation provide for the protections and participation rights of children for all digital products and services that operate in their territory. They should also join forces with regional and international organisations to ensure global standards in order that children in jurisdictions with less mature regulatory environments are offered the same protections as those in more connected societies.

49. Children should be able to understand their rights and the routes to justice therefore information should be in formats and languages that they can understand. Due to the transnational nature of online abuse, cross-border cooperation between States is crucial to ensuring effective remedies as offenders may be located in different countries to the victim. Providing information is not in itself sufficient, supported routes to justice and collective action must be provided.

[66] https://www.un.org/en/pdfs/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ENG.pdf
[67] https://d4dlaunch.eu/#about

VI. Civil rights and freedoms

A. Access to information

50. Children want, need and have the right to access information. The digital environment is a vital source of information across all fields of interest for children and States have an obligation to facilitate this access for all children. The only limitations on the exercise of the right to information arise where this is necessary to respect the rights of reputations of others or to protect national security, public order or public health.

> **"As time and technology grows, we can easily access and get information. But it's hard to know whether the information is valid or not."**
>
> Indonesia, girl, 14[68]

Uniquely the digital environment is designed in a way that means much of the information that a child views is automatically generated.[69] This creates a tension between a child's right to access and the desire (much of it commercially determined) of a business, organisation or individual to put information in front of a child, or the child as part of a wider group. In this regard a child's right to access should not be confused with a third party's desire to access or impact on the child. Children should not be made to listen or be bombarded with unwanted information.

Laws should explicitly harness mechanisms that include media and information literacy as national tools, to promote the use of the digital environment to access a wide range of quality information, recognising the digital environment's unique ability to provide information in multiple formats and in ways that are engaging and exciting for children of all ages.

51. States should use all policy levers available to them to ensure that children have access to diverse and quality information online, which prioritises social and cultural benefit and material aimed at promotion of well-being and health, over profit-maximisation.

52. States should ensure that children can access a very wide range of information from a diversity of media and other sources, including information held by public bodies. This ability to access relevant information can have a significant positive impact on equality.

[68] Our Rights in a Digital World, p. 14

[69] For example, YouTube's recommendation algorithm is responsible for 70% of the content people watch. https://www.cnet.com/news/youtube-ces-2018-neal-mohan/

Additionally, issues of specific interest to children should be available to them in their own language or formats that they understand. For example, children with visual impairments need information available in audio formats[70] and the Special Rapporteur on child trafficking has recommended the creation of child-friendly, age appropriate content for children including the provision of information on the risk of trafficking for all forms of exploitation, grooming and abuse, in the digital environment.

53. .States should support children's access to good quality information that is independent of commercial or political interests. Disinformation and misinformation interfere with these objectives.[71] Children do not have the capacity, nor should they be expected to negotiate huge quantities of false information, for example, Holocaust denial sites, health misinformation or falsehoods about public figures or social groups.[72] States should ensure that automation and filtering systems including those that business use to recommend or rank content, is of a high quality and does not prioritise content for profit or political interest.

54. The digital environment is a complex system, but this does not exempt it from the responsibilities for upholding children's rights. Information may come from individuals, including other children, from groups, including groups of children, or from organisations, businesses, or by automated means. All digital systems must regularly identify, prevent and take steps to mitigate risks to children from harmful and biased information. Many of these risks can be identified and mitigated by the introduction of a due diligence process, for example undertaking a child impact assessment and reporting findings and actions taken. These risks specifically include social media feeds and algorithms. General comment no. 16 (2013) on State obligations regarding the impact of the business sector on children's rights has further information about such processes.[73]

Mitigation should not automatically exclude children, but rather look for technological and administrative solutions. For example the introduction of legislation in the UK[74] has resulted in companies disabling direct messaging[75] (where information can be privately shared with children), introducing higher privacy settings by default,[76] stopping advertising of inappropriate activity or content to children such as weight loss and diet products,[77] investing in more accurate technology to designate the suitability of content for different age groups[78] and only age-gating for content that is clearly unsuitable such as extreme pornography or

[70] Two clicks forward and one click back, Report on children with disabilities in the digital environment, COE, 2019
[71] https://rm.coe.int/information-disorder-report-november-2017/1680764666
[72] https://www.bbc.co.uk/news/blogs-trending-38156985
[73] https://undocs.org/CRC/C/GC/16
[74] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/
[75] https://www.bbc.com/news/technology-52310529
[76] https://newsroom.tiktok.com/en-us/strengthening-privacy-and-safety-for-youth
[77] https://newsroom.tiktok.com/en-us/coming-together-to-support-body-positivity-on-tiktok
[78] https://www.theverge.com/2020/9/22/21449717/youtube-age-restriction-machine-learning-rollout-kids-content-monetization-creators

gambling and dating sites. Many of these risks are automated and amplified. States must require those who provide digital systems to ensure that they do not amplify harms.

Cyberstalking and cyberbullying are growing issues and children are the easiest and most common victims of these phenomena.[79] They are also, however, sometimes the perpetrators of such behaviour. In implementing policies and laws to address cyberbullying and cyberstalking by children, States should, to the greatest extent possible, avoid criminalizing children and should focus on restorative and educational solutions, The position of parents and legal guardians should also be considered, and they should receive support to constructively resolve such situations.

55. Content labelling is a non-intrusive way of indicating the suitability of digital content for children, in line with their evolving capacities. In addition, concise and age-appropriate information about services, the kinds of content and the moderation of content should be easily available and difficult to avoid. Making a complaint should be easy and clear to a child user.

    All content control systems should be consistent with a high bar of data minimization, for example as set out in GDPR, established in the revised German Youth Protection Act[80], and summarised by the UK's Information Commissioner's Office.[81]

56. There is no environment that is risk free for children, and many children want to access the digital environment, so protections should be proportionate and respect all rights. Too often, children's rights and needs are overlooked in the creation and deployment of the digital environment. States should ensure that legislation and regulation that protects children is in place and that digital providers comply with legislative requirements and voluntary codes of conduct to which they have committed.

    Technical controls are often used to protect children. These are only one tool and they should not be used in ways that restrict the rights to information, expression and privacy of children and adolescents. Regulatory and non-regulatory mechanisms should be added to evaluate, modify and remove them (if required).

57. States must ensure that children are able to report and make complaints without risk to their privacy or reveal their identity publicly.

[79] https://violenceagainstchildren.un.org/news/ending-torment-tackling-bullying-schoolyard-cyberspace
[80] http://dipbt.bundestag.de/extrakt/ba/WP19/2685/268540.html
[81] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

B. Freedom of expression

58. The right to freedom of expression is not dependent on any particular form of digital technology or media. The digital environment is emerging as an increasingly dominant arena for children to express their ideas, identity, opinions and political views. This may be of particular importance to children who are isolated either by their specific circumstances, refugees, in cared for settings, or by geography, rural communities or whose voices are less heard, for example due to their gender or membership of an indigenous minority.[82]

59. Any restrictions on children's right to freedom of expression in the digital environment should be exceptional, non-discriminatory and clearly articulated in language and format that a child can understand. They must also be lawful, transparent and proportionate. For example, filters should not be used to restrict access disproportionately for individual children or for groups or communities of children with particular characteristics or contexts, for example on the basis of gender or sexual orientation.[83]

    Children are participants and creators in the digital world, and while they must not be made responsible for the actions of businesses or third parties, they do need access to information and education that helps them understand their rights and respect the rights of others.

60. The experience of harassment or abuse has significant impact on children's confidence and well-being and may impact them both online and offline. This is especially true of those with intersecting identities including race, class, gender identity and sexual orientation. States should develop and implement initiatives that support a safe online environment. This includes educational and awareness programmes on digital citizenship, a broad range of support services such as helplines for victims, training for officials on protection of child human rights defenders and the collection and publishing of disaggregated data by age, gender and other characteristics on online harassment.

    States should ensure that children do not suffer from online abuse and that freedom of expression is balanced with protection from violence.

    What may be considered to be robust and healthy debate in the adult world might not always translate directly into the world of children, therefore clear guidelines need to be established which seek to map out the limits of acceptable behaviour. Such guidelines should be illustrative rather than seek to be definitive, recognising that context is fundamentally important. States should also ensure that businesses respect children's right to protection from violence that is embedded in due diligence requirements, monitoring and remedy frameworks.

[82] See for example, research in East Asia: https://www.unicef-irc.org/publications/pdf/16.EAP.pdf

[83] https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads

61. There is a need for ethical and accountable oversight of algorithmic decision-making, that ensures states protect children from automated systems that may interfere with their right to freedom of thought, or impact negatively on their development, for example recommender algorithms that may exacerbate anxieties or lead children down a path to a particular world view.

C. Freedom of thought, conscience and religion

62. Children's right to freedom of thought, conscience and religion needs to be protected in the online environment from manipulation or interference. Inferences about inner states drawn from personal data can be harmful and lead to negative outcomes or discrimination against children. Targeting and profiling based on personal data can lead to manipulation of children's inner states. Accordingly, States need to introduce data protection regulations that provide appropriate protection for children's "forum internum".[84]

    Data protections must not be limited to the information a child gives, but rather encompass all the data collected, inferred, processed and transferred about the child. As such it also offers an opportunity for setting standards and providing oversight of algorithms and automated systems. Inferences should not be made about children's inner state of mind that could be used against them.

63. States should respect and protect different forms of belief and expression and children must not be penalised for holding those beliefs. Inferences about children's beliefs should not be made in the digital environment.

D. Freedom of association and peaceful assembly

64. Children have a right to, and widely express interest in, engagement in political and social activities with others, including political demonstrations, and associations such as youth groups, sports clubs, child-led groups, political parties, and working children's organisations and movements, as well as informal association and assembly through family, friendships, and social networks, both on and offline.

> **"Today's digital age provides a platform, a voice for the minorities of a country... By means of digital tech[nology], you can keep your religion and culture alive."**
>
> Pakistan, boy, 15[85]

65. Many social, civic, political, religious and cultural activities and organisations operate partially or exclusively in the digital environment and States should consider

[84] https://undocs.org/A/HRC/28/66
[85] Our Rights in a Digital World, p. 20

guaranteeing children's right to participate in these activities, ensuring that legislation aligns equally to digital settings. Many children use digital media to organise and coordinate their civic activities, for example Fridays for Future[86], the worldwide campaign to protest against climate change on Fridays. These activities, and all those carried out by Child Defenders of Human Rights[87] must be free from surveillance and punishment.[88]

66. States should recognise the potential to create networks of children and the possibility of digital technology to have their voice heard. Children have used this technology to support their interests and to connect to each other on matters that are important to them. For example, young people in Taiwan were asked by the government to prioritise their demands in the run up to an election.[89]
States should encourage and where possible, create safe digital environments in which children can be heard.

E. Right to privacy

67. Children's right to privacy extends to privacy from the state, business, organisations, other individuals including parents and other children.

The digital environment encourages and systematises disclosure and sharing of information. This information may be provided by the child, their family or peers, and it may also be provided by institutions and organisations with which a child engages, for example school or a youth organisation. It is also both gathered, and inferred (assumed) from their digital use, for example by the search results, their use of fitness trackers, support services, or social media. Collectively this information builds a very powerful image of the child's interests, emotional state and other circumstances, which can undermine their right to privacy. Many children have little idea of the extent to which information is held about them or the ways in which it may be used to make decisions about them.

68. Data collected and processed in the digital environment is very far reaching, and, importantly, the combination of multiple sources and types of data can reveal things about a child that they themselves (and their parents) do not know, for example their sexuality, disability, or propensity for excessive use. The unintended consequences of data profiling and content recommendation can reveal very intimate details about children's lives. Over the years, there have been multiple reports of "algorithmic outing".[90] For example Netflix emphasises LGBTQ content[91]

[86] https://fridaysforfuture.org/
[87] https://www.childrightsconnect.org/children-human-rights-defenders-2/
[88] For example, a young Indian activist was charged with sedition for her alleged role in the creation of an online toolkit to organise protests against new agricultural laws in the country. https://www.aljazeera.com/news/2021/2/24/indian-climate-activist-gets-bail-in-sedition-case-over-farm-stir#:~:text=Disha%20Ravi%20was%20arrested%20in,violence%20during%20the%20farmers'%20protest.
[89] https://freedomreport.5rightsfoundation.com/a-young-democracy-is-a-strong-democracy-civil-rights-of-taiwans-children
[90] https://5rightsfoundation.com/in-action/lgbtq-children-online-why-digital-platforms-must-design-with-them-in-mind.html
[91] https://www.menshealth.com/sex-women/a29712873/netflix-algorithm-nearly-outed-gay-teenager/

or Facebook displays advertising for "coming out coaches"[92] on shared accounts or screens in communal rooms

Data protection is widely acknowledged as a tool for protecting children's autonomy, exploitation and privacy. The first standalone data protection guidance for children is the UK Age Appropriate Design Code[93], which builds on the GDPR requirement that children merit specific protections. The Irish Information Commissioner has also set out fundamentals for children's data protection[94] and other jurisdictions have announced similar intentions.

States must ensure that the way in which data is collected, processed and shared, does not negatively impact on children or violate their rights to privacy and freedom of thought.

69. In the context of the digital environment, a child is extremely vulnerable to violations of their privacy. States must set out and enforce the principles of data protection, data minimisation and a child's right to privacy in the digital environment. The right to privacy includes privacy from governments, business and other users of the digital environment, including parents.

70. States are required to create legislative and industry frameworks to protect children's privacy in the digital world. These should be systemic in nature and be transparent, accountable and enforceable. They should also be subject to review and be updated on a regular basis.

There has been considerable tension between those protecting adult privacy particularly as it regards to their privacy from the state,[95] and the abuse of that privacy by those who spread and/or consume child sexual abuse material.[96] However, the privacy offered to users, including children, by private companies must not protect those who consume or perpetrate child sex abuse nor interfere with child sexual abuse material detection systems. States must invest in measures not only to detect and take down abusive materials but must also do more to stop the uploading and spread of CSAM[97] or opportunities for predators to contact children.

Specifically, aspects of system design that encourage the creation or spread of CSAM should be identified by child impact risk assessment, for example, introducing stranger adults to children, enabling direct messaging of strangers to children, or making children's profiles public to all users, should be understood by states as

[92] https://www.intomore.com/you/facebook-ads-outed-me/
[93] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/
[94] https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf
[95] https://www.openrightsgroup.org/blog/online-harms-encryption-under-attack/
[96] https://www.theguardian.com/society/2020/dec/08/encrypted-messaging-putting-children-at-risk-of-abuse-says-watchdog
[97] http://luxembourgguidelines.org/

presenting unnecessary risks to children.[98] Equally, although many detection systems are currently inadequate, they should not be dismantled until such time as business can provide systems equal or better in the view of independent observers. Companies which are continually shown to spread or enable child sex abuse should be subject to strict legal controls and enforcement.

71. While consent from child or parent is and will continue to be one consideration in data protection, it should not be used to undermine fair and rights-respecting data protection. Any consent must be informed, meaningful and given by the person whose data is being processed, with specific implications for third party uses of children's data. It is not suitable to use data given for one purpose for a whole host of purposes that may be unclear, unwanted or unknown to the child. States should oversee the compulsory implementation of clear, short, accessible and easy to understand data use policies that cannot be changed arbitrarily without actively notifying users.

72. States should legislate to ensure that children have the right to retract, correct and delete their personal data in ways that are easy to access and understand and, that data processing does not exceeded the uses that children (or parents on their behalf) may have consented to. In all cases a child should be able to withdraw consent at any time, with a facility which is equal to that used when they first gave their consent, for example they should not have to prove their age to remove an image, if they were not asked to prove that same age and same level of assurance at the time it was created.

73. States should limit the amount of time that data can be held by public authorities or private actors and should also require the deletion of data once it is no longer required. Public bodies and private business should be subject to transparent, accountable and regularly reviewed standards of purpose limitation.

    Provisions for the transfer of data from one setting to another must address conflicts of consent between parents/carers and children, and be in a child's best interests. Consent by parents/carers should not automatically override dissent from children particularly adolescents, or vice versa.

74. Data protection is for the benefit of children and their privacy. It must be designed to observe the full gamut of their rights, for example, their right to information.

    Data is increasingly collected in all sorts of environments and from many connected devices, including, public spaces and domestic appliances, toys or wearable devices. The global connected device market is expected to grow from USD 14.3 billion in 2020 to USD 40.3 billion by 2025.[99] Surveillance (especially with the possibility of lack of consent) will amount to a violation of privacy and rights of the

[98] http://dipbt.bundestag.de/extrakt/ba/WP19/2685/268540.html

[99] https://www.marketsandmarkets.com/Market-Reports/connected-device-analytics-market-249243332.html#:~:text=%5B345%20Pages%20Report%5D%20The%20global,23.0%25%20during%20the%20forecast%20period.

child. Children may not be aware that they are being monitored while in public spaces, wearing these trackable clothes, or playing with such toys. Accordingly, States need to ensure that robust data protection measures are in place to protect children from such intrusive collection of their data without their knowledge or consent.

75. The digital surveillance of children may result in the constant scrutiny of children while online or offline, for example in educational and care settings. For example, the Covid-19 pandemic has increased the number of education settings turning to remote test proctoring software to survey if students are cheating or otherwise engaging in bad practice. Many of these services use highly invasive forms of surveillance, such as storing biometric templates of children's keystrokes,[100] tracking and monitoring students' eye and head movements and storing audio recordings of students' surroundings. Surveillance of children together with any associated automated processing of personal data, in particular where inferences are made about a child's emotional or mental state, should respect the child's right to privacy. Such invasions of a child's privacy should not be conducted routinely, indiscriminately, or without the child's knowledge, or in the case of very young children knowledge of their parent or caregiver, and where possible they should have the right to object to such surveillance.

76. Concerns about the dangers of the digital world have resulted in a growing market of surveillance tools that monitor children's devices, track their location or make what they are doing online available to others, primarily parents or educators. These tools should be used sparingly and only for well-defined purposes, as they may give a false sense of security, interfere with a child's development by creating the impression that they are never alone and inhibit the development of social and critical skills to support their own safety and autonomy. They may also create tensions between parents and older children, as they form views and experiences of their own.

77. Anonymity is a very contested feature of the digital environment. It can offer privacy for children who may otherwise be prevented from or punished for speaking out, but it might also protect those who bully, abuse, promote hate or spread misinformation. States should encourage a safety-by-design and privacy–by-design approach. By considering anonymity as part of a balance between safety and privacy it is possible to engineer more nuanced approaches more suited to individual environments. For example, the identity of account holders can be verified with the services even if the identity of the user is not made public, allowing business to contact or block those who break community rules.

    Some children use online avatars or names that protect their identity, and such practices can be important to protect children's privacy. For children who are same

[100] https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education

sex attracted, intersex or gender diverse, privacy and anonymity online can also provide protection from persecution as they explore their identities.

78. States must ensure that children who access counselling and other health support can do so regardless of their age without requiring the consent or permission of an adult, including their parents. States should ensure that health and counselling services accessed by children, meet high standards of privacy, confidentiality and child protection. A child must not suffer a violation of their other rights as a result of seeking advice or help.

F. Birth registration and right to identity

79. For many children having access to identity documents is necessary to access state services. Digital technologies offer a vast opportunity to extend the provision of birth registration and in doing so extend access to services particularly for those children who may live in isolated communities, on the move or separated from family.

States should promote birth registration schemes and ensure that information about how to access them is widely disseminated. These schemes should be privacy preserving and not be used to discriminate, punish or in any way violate the other rights of children.

VII. Violence against children

80. Increasing amounts of time on virtual platforms can leave children more vulnerable to online sexual exploitation and grooming. There has been a consistent rise in screen time, which together with a lack of face-to-face contact with friends and partners, may lead to heightened risk-taking such as sending sexualized images. Decreased facilities that support meeting face–to-face, and greater dependence on time online using products and services that are primarily designed with adults in mind can expose children to potentially harmful and violent content as well as greater risk of cyberbullying.

> **"The internet allows for broader discussions about existing violence, but it increases the possibility of violence, such as cyberbullying."**
>
> Brazil, girl, 15[101]

Additionally, the digital environment opens up new ways for sexual offenders to solicit children for sexual purposes, participate in online child sexual abuse via live

[101] Our Rights in a Digital World, p. 36

video streaming, distribute child sexual abuse material, and commit sexual extortion of children, including by illegally and secretly accessing cameras, microphones or personal files on computers or mobile devices.

81. The growth of child sexual abuse and exploitation online is an issue of very considerable concern across all agencies working with children. There are a number of important documents already in place providing guidance on measures necessary to address such abuse and exploitation including:

- General comment no.16 (2013) on State obligations regarding the impact of the business sector on children's rights[102]
- General comment no.13 (2011) on the right of the child to freedom from all forms of violence[103]
- General comment no.14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)[104]
- Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises (2008)[105]
- Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011)[106]
- Report of the Working Group on the Universal Periodic Review – Rwanda (2011)[107]
- CRC Report of the 2014 Day of General Discussion, Digital media and children's rights[108]
- Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children child prostitution and child pornography (2019)[109]

Violence against children is not restricted to strangers nor to sexual violence. Many children are violated by people known to them, including family members, and many children suffer from one or more forms of violence including those that are promoted by content online, such as self-harming, suicide or extreme eating behaviours.

Strong preventative measures should be introduced for all forms of violence and digital businesses should have effective and transparent forms of moderation,

[102] https://undocs.org/CRC/C/GC/16
[103] https://undocs.org/CRC/C/GC/13
[104] https://undocs.org/CRC/C/GC/14
[105] https://undocs.org/A/HRC/8/5
[106] https://undocs.org/A/HRC/17/31
[107] https://undocs.org/A/HRC/17/4
[108] https://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf
[109] https://undocs.org/CRC/C/156

report and response in environments in which violence takes place. A victim searching for help must be protected from being confronted with images of child abuse or offender forums. The use of safety technologies should be encouraged in a targeted way that blocks the most serious risks and illegality but does not inhibit a child's ability to access information and support.

Not all children react in the same way to the same circumstances and many smaller acts of violence lead to more extreme ones. States should consider all acts of violence against children, including facilitating acts of violence, as a violation of a child's right to protection.

82. The multifaceted and complex challenges resulting from online violence against children require States to establish holistic and up-to-date legal, institutional and practical prevention, care, assistance, support and protection mechanisms, including special police units, well-equipped and trained specialized justice system actors, along with child-friendly reporting and investigation mechanisms, and accessible helpline services.

There is a key role for the education system, including non-formal education, in fighting online violence, peer violence, bullying and harassment in schools. States should develop specific curricula, train and equip teachers and other education personnel with pedagogical tools, referral focal points within schools for reporting such incidents and mechanisms to investigate in coordination with the social system, the police and the justice system. Teachers should not be left without resources or training programmes that are comprehensive and free of commercial interest.

Business enterprises should meet their responsibility to protect children effectively from all forms of violence by reforming business practice, developing technical tools, taking advantage of the latest available knowledge and innovations and by taking a proactive and preventative approach to system design. For example, Photo DNA is freely available but still many companies do not use it.[110]. Without prompt and preventative action, platforms have been used to spread hate and violence, for example in Myanmar.[111] States should develop regulatory approaches that require industries to take all reasonable and proportionate technical and procedural steps to combat criminal and harmful behaviour directed at children in relation to the digital environment. These requirements should be subject to legal safeguards that protect other fundamental rights such as the right to privacy and the right to freedom of expression.

83. The digital environment opens up new ways for criminal groups, including gangs, to solicit and traffic children for criminal purposes, including to distribute drugs. Social media services such as WhatsApp have been used heavily as a recruitment channel

[110] https://www.iicsa.org.uk/publications/investigation/internet/part-c-indecent-images-children/c2-detection-images
[111] https://resourcecentre.savethechildren.net/node/16212/pdf/mobile_myanmar_2019_2019-11-06.pdf

for children[112]. Geolocation tracking such as 'Find My Friends', as offered in different smartphones, is used to monitor and track children's movements as they transport and sell drugs across the UK, where children are sometimes forced to livestream their movements 24 hours a day.[113]

States should ensure that anti-trafficking legislation prohibits the recruitment of children by criminal groups, and that child offenders are treated as victims or, if tried, in accordance with child friendly justice systems. States are encouraged to fully incorporate the non-punishment principle, as elaborated by the UN Inter-Agency Coordination Group against Trafficking in Persons (ICAT),[114] to ensure a more consistent, human rights-based application of the principle, which provides that trafficked persons should not be subject to arrest, charge, detention, prosecution, or be penalized or otherwise punished for illegal conduct that they committed as a direct consequence of being trafficked.

VIII. Family environment and alternative care

84. Parents and caregivers need support in understanding the ways in which digital technologies and businesses impact on children. These include the ways in which children can realise their rights using digital technology, as well as the ways in which they may be at risk or come to harm.

Digital systems should be designed in recognition of the fact that many children do not have the support of parents who are engaged, literate or skilled in digital technologies, and therefore systems should be privacy preserving, safe, supportive and age appropriate by design.

85. States should provide realistic support for parents that recognises time, emotional, cognitive and literacy pressures in domestic contexts. Parents often have their own issues with technology and the emotional, empathic and affective technologies aimed at children are also likely to affect parents. This may at times have a profound effect on their role as parents and within family dynamics. For example, children report that parents are often distracted by their own smart phones or that they find distressing material on devices shared with parents.

States need to pay particular attention to imposing standards on products and services that parents are unlikely to be well informed about, for example the data collection and downstream use of persuasive techniques.

Children use digital products and services at increasingly young ages. Parents may be unaware of the nature and impact of many services and take a time-based

[112] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf

[113] https://www.theguardian.com/global-development/2019/feb/05/county-lines-drug-gangs-blackmailing-tracking-children-social-media

[114] https://www.unodc.org/documents/human-trafficking/ICAT/19-10800_ICAT_Issue_Brief_8_Ebook.pdf

approach to children's use, rather than one that responds to the nature of the product and service, and the evolving capacities and circumstances of their child.

If children are overly restricted it impacts on their willingness to report negative experiences, even encouraging them to evade scrutiny or engage in deception. States should support parents by providing sophisticated information, free of commercial influence, that helps them understand the multiple risks and opportunities their children face. Positive parenting techniques, including enabling and supporting children to use technology wisely, are vital.[115] Information and education are an addition to, not replacement for, systemic risk assessment and mitigation strategies to ensure that the digital environment is safe by design.

86. Parents and children express the desire for parents to have a greater understanding of the digital environment as well as the skills to engage with it. Advice should be given in a manner that recognises that families have a wide range of cultural and personal views and that children as they grow older will have their own independent views.

States should give advice that encourages children's access to and safe use of the digital environment for a wide range of activities. Parents should be supported to develop skills and knowledge of digital technologies, including how to support their child's positive use of a broad range of rights-respecting products and services.

87. States may have to make specific interventions to ensure that children separated from their families have access to digital technologies to maintain contact. This may include children of parents or caregivers working abroad or in different parts of the country, parents who are incarcerated or children who live with other members of family or who are themselves in alternative care.

Such access may require a wide range of considerations, for example, investment in infrastructure, electricity, access to devices, data, or the circumstances and permissions to make contact.

88. Contact must be in the child's best interests. For example, it must not be a route for abusive parents to reconnect with children from whom they have been separated. Welfare services may need to supervise such communications, and for this they must be trained to understand the risks. For example, digital technologies have the facility to pinpoint a child's location or broadcast personal information that makes their interests or habits visible to many millions of viewers. Safety-by-design principles[116] should take in to account the vulnerability of children to adults, including family members, who pose a risk.

[115] https://www.unicef.org/parenting/
[116] https://www.esafety.gov.au/about-us/safety-by-design

IX. Children with disabilities

89. The digital environment offers a world of opportunity to children with disabilities. For example, for children who require mobility support, digital location imaging can help them find out if an area is a wheelchair accessible.[117] Google Maps, for example, collates wheelchair accessibility information for more than 15 million places globally.[118] However, in order to benefit from these opportunities, it is important for States to identify any barriers that children with disabilities may face in accessing digital technology, for example, through software design, inaccessible websites, services and applications, lack of adaptations, or financial difficulties, and take all necessary action to address and remove these barriers.

90. States must consider and act upon the rights of children with disabilities to access the digital environment. Accessibility strategies, availability of assistive technologies, and standardisation of an accessible online environment all offer rich possibilities for greater access. States should ensure access to a wide range of affordable assistive technologies and ensure that the provision of digital services does not restrict access to physical and virtual engagement for children with disabilities, especially those living in poverty.

    States should provide guidance and resources to staff in schools and other relevant settings so that they have sufficient training to rethink school dynamics and methodologies when the needs of children with disabilities are not being met. Further, the States should guarantee the availability of the contents of compulsory formal education in virtual format through materials and technologies appropriate to the special needs of children with disabilities.

91. In creating digital systems that are accessible to children with varying needs, states should engage with, and encourage business to engage with children themselves. Children have views about how the digital world could be better designed for their use.

> **"[We need] youth friendly terms and conditions with a summary of the most relevant points."**
>
> Germany, boy, 17[119]

92. While the digital environment offers specific opportunities for children with disabilities, it is the case that those same children often face greater risk,[120] including greater risk from child sexual abuse. States should ensure that the

[117] https://publications.parliament.uk/pa/cm201719/cmselect/cmpetitions/759/75905.htm#footnote-117

[118] https://blog.google/products/maps/wheelchair-accessible-places-google-maps/

[119] Our Rights in a Digital World, p. 15

[120] https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f

enhanced risks faced by children with disabilities should form an integral part of child risk assessments and safety by design programmes. Information provided for children, should be provided in accessible formats.

States should support the development of child-led organisations and initiatives of children with disabilities and their active engagement through the digital environment, as well as support adults in facilitating such initiatives. For example, the Council for Disabled Children[121] supports members' participation in online advocacy.[122]

X. Health and welfare

93. Digital products and services should be developed to increase access to health and wellbeing services for children, including in times of public emergency or crisis. For example, in 2019-20 many organisations have developed information resources on Covid-19 for children,[123] and for adults to talk to children.[124]

94. Children use digital services to access health information, including sex and reproductive information. States should ensure that services that offer such information do so in a way that is of a high quality and does not compromise the privacy or confidentiality of the child. In particular, data protection must be in place for services that offer health advice to children. For example, under the General Data Protection Regulation (EU GDPR), Privacy International asked five different menstruation apps to share the information they held on users.[125] These apps were based in Germany, India, the British Virgin Islands, and the United States. Their investigations found that of the five apps surveyed, only two apps responded to requests for data information under the Data Subject Access Request (DSAR). Of these two, multiple pages of sensitive data, including data about a user's sexual life and habits and medication intake were stored on the app's servers. Some of this data was also shared with third parties.

    Professionals working in health and welfare services (e.g., professionals at maternity clinics) play an essential role in helping children, young people and families take care of their digital wellbeing.

95. Digital technologies should enhance a child's access to health provisions. A child should not suffer violations of their other rights, for example their right to privacy or to have their views heard in matters that affect them.

[121] https://councilfordisabledchildren.org.uk/our-work/participation
[122] https://www.un.org/development/desa/disabilities/
[123] https://www.unicef.org/romania/covid-19-information-children-adolescents-parents-and-professionals
[124] https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/talking-with-children.html
[125] https://privacyinternational.org/long-read/4316/we-asked-five-menstruation-apps-our-data-and-here-what-we-found

> **"I researched about mental illness, depression and anxiety, out of curiosity, because nobody talked about it and I wanted to know more."**
>
> Brazil, boy, age unknown[126]

States should ensure that the introduction of digital products and services into the health sector does not discriminate against certain groups of children by denying them access to in person health care, or a lesser quality of service because it is provided online.

96. There are health risks associated with the use of some products and services and the risk of harmful health information spread by digital services, for example, a rise in self-harm as a result of its widespread coverage on social media,[127] or the prevalence of misinformation and disinformation about vaccinations.[128]

States should anticipate the needs of children by encouraging safety by design regimes as a norm, and by putting in place sufficient regulatory and legal frameworks to ensure the safe participation of children in the digital environment. For example as part of the UK government's upcoming Online Safety Bill, the government will establish a new statutory duty of care to require services to anticipate the safety of their users.[129]

97. Digital services and products can be used to encourage healthy behaviours, exercise, contact with others, civic engagement and learning. These should be encouraged but not at the expense of children's other rights. States should put in place regulation that prevents children being targets for unhealthy or age inappropriate products, and protections children are afforded offline must be embedded online. For example, embedding the World Health Organisation Guidelines on Food Advertising,[130] into regulation.

98. Guidance for parents, children and educators should encourage the productive and enjoyable use of digital technologies, whilst recognising that child development requires a balance of activities. The digital world is designed to maximise attention, interaction and constant engagement – children need time off as well as time on and states should make clear in their guidance that children have a right to rest, which is a crucial developmental requirement.

[126] Our Rights in a Digital World, p. 38
[127] Arendt, F., Scherr, S., & Romer, D. (2019) Effects of exposure to self-harm on social media: Evidence from a two-wave panel study among young adults. https://doi.org/10.1177/1461444819850106
[128] Buri, T. (2019) Vaccine Misinformation and social media. https://doi.org/10.1016/S2589-7500(19)30136-0
[129] https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper
[130] https://www.who.int/dietphysicalactivity/marketing-food-to-children/en/

XI. Education, leisure and cultural activities

A. Right to education

99. Traditional education delivered by digital means creates the prospect of greater access to a quality education and associated learning activities. Increasingly, digital literacy is an essential skill and represents a vital contemporary extension of the right to education, requiring States and educational and cultural institutions to make appropriate provisions for the development of digital skills to further the education and participation of children and adolescents in the digital environment.[131]

The realisation of children's rights to information necessitates access to quality online resources to support their learning, along with the acquisition of the digital skills necessary to develop the "personality, talents and mental and physical abilities" of children and adolescents for a responsible life in a free society.

100. Educational and cultural institutions such as archives, libraries and museums can use digital technologies to support children to engage with their own creative and cultural practices and to learn about those of others, through the means of global education.

101. All schools need to have an adequate technological infrastructure that enables every child to benefit fully from the digital environment, and this needs to be backed up by properly trained teachers and quality programmes.

States should make deliberate efforts to address digital divides when they are working to uphold the right to education. As online learning becomes embedded in education states need to take account of children from different backgrounds and situations. Remote or other online learning activities should not create additional burdens or inequalities for children, who do not have digital access, skills, and support. States should ensure that accommodations are made for children with disabilities, including accessibility of ready-made content using subtitles and verbal description of visual content, allowing additional accommodation such as using sign language and linguistic simplification, making digital learning accessible, in accordance with the pupil's needs, and adopting universal accommodation principles.

In order to support a rich learning environment States should ensure that copyright protections have appropriate exceptions for materials used for educational purposes.

[131] https://en.unesco.org/themes/media-and-information-literacy, https://www.unicef.org/globalinsight/media/1271/file/%20UNICEF-Global-Insight-digital-literacy-scoping-paper-2020.pdf

102. For children attending school (or nursery, college, or other educational institutions), digital educational technologies can support engagement between teacher and student and among peer learners. For children not physically present in school or living in remote areas or in disadvantaged or vulnerable situations, digital educational technologies can enable distance or mobile learning programmes.

States should create a digital environment that can ensure that children continue to have access to education without being interrupted in cases of emergencies, natural disasters and epidemics (such as what the world is currently witnessing in light of the pandemic Covid-19); and to respect the needs of children and their families in this context. For example, during the Covid-19 pandemic, Bangladesh's government broadcaster has been airing recorded classes on its channels. The decision to turn to television and radio for those with no internet-enabled devices or broadband access has proven more successful at reaching a large percentage of children.[132]

States should ensure and provide children that cannot attend classes in person at schools with access to connectivity resources (internet, computer, tablets, etc.) that allow them to receive education in a digital environment. Additionally, States should implement a plan, to the maximum of their available resources, to guarantee fair access (both inside and outside school) to these resources for every child physically attending.

States' responsibilities must ensure that schools have sufficient resource to provide parents with guidance on online home schooling and learning environments. This should also include guidance on protecting against the risks that come with using digital technologies.

103. Standards for digital educational technology should ensure that uses of these technologies safeguard children's rights and do not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights, including the use of digital technology to document a child's activity and share it with parents without the child's knowledge or consent.[133]

104. It is critical that digital literacy education educates children about the design and purpose of the digital world and an understanding of children's rights including their application in the digital environment. Education that addresses these key areas should be co-designed with children and experts and available to children formally through education settings.

---

[132] https://www.bbc.co.uk/news/world-south-asia-54009306

[133] For example, police will be able to access data collected by Singapore's contact tracing app, Trace Together (which is used by nearly 80% of Singapore's 5.7 million residents), for use in criminal investigations. This is a contradiction to the privacy policy initially outlined when the government launched its app in March 2020, after saying participation in contact tracing is mandatory.
https://www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid/

The introduction of digital literacy education should begin in early childhood, or as soon as children begin using technology. States should support kindergartens and day care centres in equipping children with the skills and knowledge they need to stay safe online and to engage beneficially with the digital environment.

Education should include a critical and information literacy component, to support searching for and evaluating reliable information, including health information and sensitive information sought by children on a confidential basis as needed, to support well-being and a healthy lifestyle. The Australian Government offers a strong example of this in their parenting website.[134]

Digital literacy programmes should include equipping students with the knowledge and skills to handle safely a wide range of digital tools and resources and those related to content, creation, collaboration, participation and civic engagement. They also need education in how to critically evaluate sources of information to enable them to differentiate between trusted or reliable sources of information and misinformation and other forms of biased or false content, and to participate as engaged actors in their communities.

Digital literacy curricula should cover a comprehensive set of topics, including how digital services can help them access confidential support and advice on a broad range of issues, for example sexual health and mental health. Safety curricula should also emphasis positive engagement in the digital world particularly how they might safely meet and work alongside other children on matters that their security and safety online and off. For example, many young people across the globe have used the digital environment to organise collectively to express their views and their fears about climate change.

The sustainable development goals offer a vision of a world in which skills, values and attitudes necessary for the transition to a more sustainable and equitable relationship with the worlds resources, Children should be taught about the role that digital technologies can play in promoting, or on occasion, detracting from this journey. States should promote the implementation of education for sustainable development (ESD) to enable a critical, resilient and responsible handling of digital technologies, practices and contents.

Online safety curricula should support children's engagement online by encouraging debate and knowledge about respectful behaviour; children should be able to identify abusive interactions, their own and others. All programs should aim to equip students with knowledge about human rights, including the rights of the child and of others in the digital environment, and available forms of support and remedy.

States should invest in training to ensure that teachers are equipped to teach comprehensive digital literacy courses.

[134] https://raisingchildren.net.au/

105. Students should be taught at least rudimentary cybersecurity and digital safety from the ages at which they first begin to use digital technology. They should also understand the social, economic, cultural, political and environmental implications of digitalization and surveillance.

Teachers should be trained to provide this education and should have a broad knowledge of data practice and business arrangements of the sector as well as a rich set of resources to guide the beneficial use of diverse digital products and services.

> **"We would like the government, technology companies and teachers to help us manage untrustworthy information online"**
>
> Ghana, group of children[135]

B. Right to culture, leisure and play

106. Online and offline play are a vital dimension of the joy of childhood and an essential aspect of children's development. Children from all over the world emphasise the value they attach to the interest, fun and stimulation they gain from online activities. However, play is too often perceived by parents as 'non-productive', in which children are simply wasting time. States should encourage the beneficial use of the digital products and services and encourage parents to understand the value of play in the digital world. For many children, playing online offers opportunities to collaborate, experiment, create and explore that they greatly enjoy and benefit from, and that may be otherwise lacking to them. Especially if designed in ways that respect children's rights, the digital environment can provide stimulating spaces and resources that supports free play in ways that children find emotionally and culturally meaningful.

107. The digital environment has an increasingly important role in shaping the individual and community identities of children. Children utilize online spaces in constructing, exploring, and expressing their identities. There is a danger that content available in the digital environment is predominately in English and concentrated in the cultural experience of those who build and own it, primarily the US. States should encourage and invest in local content in the languages that children speak,[136] recognising that children will benefit from and form their identity as a result of their engagement in a wide range of cultural and civic activities online.

[135] Our Rights in a Digital World, p. 14
[136] Researchers have found that Spanish-language content is less often and less quickly moderated for misinformation than English content. While 70% of misinformation in English on Facebook ends up flagged with warning labels, just 30% of comparable misinformation in Spanish is flagged.
https://secure.avaaz.org/campaign/en/facebook_coronavirus_misinformation/

108. The vast majority of the digital world is made by adults for use by adults, with the result that children are often left in a world that is not designed with them in mind. States should encourage digital products and services that are designed specifically for children and where children access adult products, providers must consider the needs of children. The digital environment represents an unparalleled opportunity for leisure and learning, but it must be designed to respect children's rights and meet their development needs.

109. Children need a balance between play and leisure in online and offline spaces, and face to face interaction is essential for all aspects of their development. As much as children enjoy and embrace digital life, meeting friends, families and accessing services in the places they live is also important to them. In particular, recreational activities such as games, socialising, participation in group activities and sports in the physical environment are important for their health, wellbeing and happiness.

110. Children can be harmed in the digital environment when, in order to engage in a game or activity, they are targeted by advertising (for example, for unhealthy food), pushed by persuasive design techniques, or encouraged to give up their personal data. The influence and impact of such techniques is such that the World Health Organisation made the reduction of children's exposure to marketing of unhealthy foods one of the core recommendations of their Commission on Ending Childhood Obesity.[137] States should regulate to ensure that children are offered protections from the aggressive commercialisation of childhood.

111. It is important when introducing regulations, to find a balance between providing adequate protection for children from harmful content and the freedom to explore opportunities for play, recreation and leisure online.

XII. Special protection measures

A. Protection from economic, sexual and other forms of exploitation

112. States must protect child victims of online sexual exploitation and abuse by ensuring that harmful material such as child sexual abuse material is actively investigated, identified and removed. This is to ensure that child victims of online child sexual abuse are identified, taken out of situations of abuse, and that they can access justice, remedy and necessary social and psychological support.
For this to occur, national coordination and specialized training within law enforcement is necessary, adequate funding must also be allocated, and states must cooperate internationally.

[137] https://www.who.int/end-childhood-obesity/en/
https://www.euro.who.int/__data/assets/pdf_file/0017/322226/Tackling-food-marketing-children-digital-world-trans-disciplinary-perspectives-en.pdf

113. States should regulate and enforce existing laws concerning artistic child labour, characterized by habitual, monetized or rewarded and performance-oriented with external expectations involvement of children in artistic or entertainment productions, with the appropriate protections stipulated, such as judicial authorization, educational and psychological accompaniment, and working day limits, as stipulated by the Convention No. 138 and the Recommendation No. 146 of the International Labour Organization, recognizing its relevance to child digital influencers. For example, France has passed a law on the commercial use of child influencers' images on online video sharing platforms if the child is under the age of 16.[138] These new protective measures will include child digital influencer under the remit of French labour codes, where compensation for child digital influencers will qualify as a salary.[139]

States should also review relevant laws and policies to ensure that children are protected against economic and other forms of exploitation, and that their rights with regard to work in the digital environment and related opportunities for remuneration are protected. States should also inform parents and children about protections that apply and ensure that appropriate enforcement mechanisms are in place. The digital artistic labour shall not be illegally exploited nor used as a means of targeting commercial content to other children. States should also inform parents and children about protections that apply and ensure that appropriate enforcement mechanisms are in place.

States must also work to address the role that child exploitation plays in the production of digital devices such as smartphones, laptops, and electric cars. For example, investigations have uncovered the presence of children working in unregulated conditions in the Democratic Republic of the Congo (DRC).[140]

114. States must ensure that laws and regulations are in place to protect children effectively from harmful goods or services that they may encounter online. These laws must be backed up by the necessary resources and commitment to enforce them.

Businesses who sell or make available age restricted goods and services need to employ age verification mechanisms that provide appropriate levels of safeguarding, privacy and data protection.

115. Laws that cover child trafficking must be updated to cover the digital environment, for example the United States House of Representatives bill, Fight Online Sex Trafficking Act (FOSTA) and the United States Senate bill, the Stop

138 https://www.bbc.co.uk/news/world-europe-54447491

139 https://marketinglaw.osborneclarke.com/data-and-privacy/french-parliament-adopts-law-commercial-use-child-influencers-image-video-sharing-platforms/#:~:text=The%20French%20Parliament%20adopted%20an,Youtubers%20count%20millions%20of%20subscribers.

140 https://www.oecd-ilibrary.org/docserver/5d3abe03-en.pdf?expires=1615902487&id=id&accname=guest&checksum=60206F84B1815E701A64A522AE238C79

Enabling Sex Traffickers Act (SESTA), signed by President Donald Trump.[141] The FOSTA-SESTA package makes it illegal to knowingly assist, facilitate, or support sex trafficking, including the sexual exploitation of children. States should ensure that digital services and products do not either intentionally or unintentionally foster or hide child trafficking.

116. Each jurisdiction or region may have its own laws, general comment no. 25 sets out the expectation that they will be updated to cover the digital world. In the UK for example, the introduction of a statutory code under the Data Protection Act 2018 to set standards for online services to protect children online – the Age Appropriate Design Code.[142] Or in Ghana where children are specifically cited in the 2012 Data Protection Act.[143]

B. Administration of child justice

117. Children who are arrested and prosecuted for cybercrimes should receive the full protections of child justice systems as set out in general comment no. 24 (2019) on children's rights in the child justice system.[144] This includes terrorist-related offences that are alleged to take place in an online settings for example, children are increasingly at risk for the crime of 'glorifying terrorism'.[145] Cybercrimes can often effectively be addressed through the use of restorative justice mechanisms. Where applicable, pre-trial diversion processes must be available to child offenders with supervision and rehabilitative training on the responsible use of digital technologies.

States should seek to use digital technologies in ways that support children's access to justice.

118. The rise in self-generated content is associated with a number of norms of the digital world – for example popularity metrics that encourage young people to spread images that will get disproportionate engagement or the commercialisation of sexual content by influencers.[146]

Children do not have adult capacity nor responsibility and should not be criminalised for creating such content, but states should instead respond to this behaviour, some of which is generated under coercion, by providing children with the education and emotional support needed for their rehabilitation. Safety by design frameworks

[141] https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom
[142] https://ico.org.uk/for-organisations/age-appropriate-design/additional-resources/what-is-the-children-s-code/#:~:text=The%20Children's%20Code%20(or%20Age,comes%20to%20their%20personal%20data.
[143] https://iclg.com/practice-areas/data-protection-laws-and-regulations/ghana
[144] https://undocs.org/CRC/C/GC/24
[145] https://www.trtworld.com/magazine/french-police-interrogate-muslim-children-for-disliking-insulting-cartoons-41233
[146] For example, OnlyFans, a subscription-based service allowing the sale and purchase of sexually explicit content, has become more mainstream for celebrities and social media influencers. Because of this celebrity-status, children have been both exposed to content stemming from OnlyFans (for example, because creators promote OnlyFans content on services such as Twitter, which allow nudity on their platform), as well as the idea that one can achieve financial success from the service. In this way, children are at risk from both accessing pornographic content, as well as unintentionally participating in the solicitation and production of child sexual abuse imagery when sexual content has been commercialised and advertised in the digital world.

should ensure that digital services do not enable and encourage the creation of self-generated sexual content.

119. Surveillance in public places should not be used to prosecute children or deprive them of other rights – for example the right to association. In the summer months of 2020, protestors gathered around the world in solidarity with the Black Lives Matter movement. There is concern that digital surveillance, from police use of facial recognition software and public videos or images uploaded of protestors, could leave many people unknowingly part of facial recognition databases.[147]

120. Where the digitalisation of court proceedings results in a lack of in-person contact with children, it may undermine the child's ability to meaningfully engage with the courts and, within the criminal justice system, and frustrate rehabilitative and restorative justice measures built on developing relationships with the child. Remote court proceedings may be disorientating or deprive children of in person support that they need.

AI introduced into the justice system may have discriminatory effects or violate children's other rights, a precautionary principle should be followed to prevent violation of the right to non-discrimination and of privacy in the context of AI.[148]

States should ensure that the roll out of digital services in justice settings does not undermine children's rights or alienate them from the process of justice. Where children are deprived of their liberty, in person contact is equally necessary to ensure the well-being and rehabilitation of children.

C. Protection of children in armed conflict, migrant children and children in other vulnerable situations

121. The digital environment can empower children and others with valuable information about situations during armed conflicts, seeking asylum, and natural disasters which may be the difference between life and death. It can enable them to maintain contact with families, seek vital information, obtain help, continue with education, and feel connected with the outside world. In some cases, the digital environment can even be an escape from the realities of armed conflicts, as demonstrated by the popularity of video games for young people in Afghanistan.[149] Issues like commercial (or non-commercial) exploitation of vulnerable children from such environments must be considered by governments – photography, videography, drone surveillance, or other such modes for activities like documentary-making etc.; especially when non-consensual is a grave violation of the rights of these vulnerable children.

147 https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database
148 https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf
149 https://www.nytimes.com/2020/11/23/world/asia/afghanistan-video-games-pubg-playerunknown-battlegrounds.html

Intergovernmental social cohesion programs for the digital environment should be considered and designed in order to overcome the problems faced by children in armed conflict, migration and other vulnerable situations (to improve life skills, to minimise social adaptation problems, to increase their awareness of risks and resources in society, to ensure that they live a life in accordance with their rights and at the same time to develop mutual understanding and tolerance between cultures).

122. The digital environment has allowed for grooming of children by extremist groups to become radicalised and involved in armed or violent conflict both domestically and internationally. For example, German citizen Linda Wenzel is just one of dozens of children groomed and recruited through digital communication at 15 years old to go to Syria from Germany to join ISIS.[150] States should ensure that such activity is criminalised and effectively investigated and prosecuted.

XIII. International and regional cooperation

123. The international nature of the businesses that provide digital services and products creates a need for bilateral and multilateral cooperation. While individual states have a responsibility to protect children within the confines of the legislation of the country in which they live, states should collaborate for the purposes of law enforcement, in order to share information, and to create consistent standards. If such measures were international or regional they would be better placed to protect the full gamut of rights, such as freedom of expression or the right to information, whilst tackling disinformation and hate speech.

124. The digital word is international in nature and therefore cooperation between states is encouraged. Many states have begun the process of creating standards and regulatory regimes in one or more areas covered by the General Comment. Knowledge sharing and adopting common approaches has the potential to speed up and support greater provisions and protections for children across the globe. Cooperation may be on a regional, international and bilateral basis. In particular, the adoption of common language and definitions will ensure smooth cooperation across borders. For example, the Universal Terminology of the Model National Response on child sexual abuse.[151]

[150] https://www.independent.co.uk/news/world/german-isis-bride-death-penalty-hanging-iraq-groomed-teenager-linda-wenzel-a7984171.html
[151] https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf

XIV. Dissemination

125. The content and recommendations of the GC will have greater value if they are widely known about and understood. States need to make significant efforts to ensure that everyone for whom it is relevant has access to it and is supported to understand what it means and what action needs to be taken in response. Child friendly or accessible versions should also be made available and distributed very widely throughout society.

Appendix 1: Glossary

Term	Definition
Assistive technology	Technology developed to support or improve an individual's independence, including adaptive and rehabilitative systems and devices for people with disabilities such as a screen reader or speech recognition.
Automated processing	The process of making a decision by automated means, i.e. using software configured to analyse the data provided and to follow set rules to reach decisions based on algorithms, without human involvement.
Automated search	The process of assessing user data to filter the content they access online, primarily for commercial interests. Content is usually chosen based on perceptions of the user's reaction to other content, or based on content that other users who acted in similar ways went on to seek out.
Automated systems	Software and hardware programmed to perform a function automatically without the need for human intervention to provide inputs and instructions for each operation.
Behavioural targeting	Analysing users' online activity in order to target them with advertising, messaging, suggestions for further content or contacts with other users based on their previous preferences, often with the intention to manipulate their future behaviour.
Content, contact, conduct and contract risks	Content risks: Potential harm to users based on the nature of online content, including age-inappropriate (e.g. pornography), unreliable (e.g. misinformation or disinformation) or certain other categories of content (e.g. promoting risky behaviour or methods of self-harm or suicide). Contact risks: Potential harm created by the opportunity for users to contact each other using online services, e.g. enabling strangers or people hiding their identity to contact children. Conduct risks: Potential harm based on the behaviour or conduct of the user or their peers, e.g. deliberately using online platforms to threaten or harass other users, including cyberbullying, "sexting" and hateful comments, sometimes also unintentionally by disclosure of private information of other users. Contract risks: Potential harm wherein a user is exposed to inappropriate commercial contractual relationships or pressures, e.g. compulsive use, gambling, targeted advertising, hidden costs, unfair terms and conditions, and loss of control of personal data.
Content moderation	The practice of monitoring and reviewing user-generated content against pre-determined rules to remove content deemed

	impermissible, either automatically or using human moderators. Content moderation can be performed simultaneously with content generation, as in chat services or with a time delay, as in forums.
Cyber-aggression	Acts of harm enacted by individuals or groups, online or through the use of digital technology, often with the intention of causing offense or hurt to another individual or group.
Data minimization	The principle of only collecting the minimal amount of relevant personal data necessary to the purpose for which it is being processed, and retaining that data only so far as it is necessary to the purpose.
Data processing	Includes processes of data collection, recording, retention, analysis, dissemination and use.
Digital literacy	The ability to use information and communication technologies to find, evaluate, create, and communicate. Related terms include 'media literacy', 'information literacy' or 'media and information literacy', among others.
Digitization	The adaptation of environments, practices, businesses and daily life to include and benefit from digital services and infrastructure. This also refers to the conversion of information into a digital format.
Disinformation and misinformation	Disinformation: When false information is knowingly shared. Misinformation: When false information is shared, but no intentional harm is meant.
Emotional analytics	The collection of data to determine or infer an individual's mood, often conducted by assessing video, voice and written communication, or personal data, to identify markers such as facial expression and tone that are correlated with specific emotions using machine learning techniques including algorithms.
Identity theft	The fraudulent impersonation of another individual, e.g. in order to access their wealth, damage their reputation, gain access to their online contacts or otherwise profit.
Immersive advertising	The seamless integration of advertisements into online content or digital services, allowing users to remain immersed in the content and services features whilst simultaneously being exposed to brand marketing and messaging.
Implant technology	A microchip that can be implanted into a person to store, track or retrieve information contained in an external database, such as 3 personal identification, and/or medical or law enforcement or contact information.

Information filtering	The use of a programme to screen digital content and identify or hide content that matches set criteria. Common uses of information filtering include hiding offensive content from appearing in search engine results, or sorting which results appear first.
Interoperability	The ability of different systems to communicate with each other, share data and make use of received information.
Neuromarketing	The study of how people's brains react to marketing content, and the application of this in developing more effective marketing campaigns. Reactions can be measured in a wide range of ways, from brain activity scanning to engagement time, click-throughs and time spent on a website.
Privacy-by-design	The practice of designing online services with the aim of protecting users' privacy as much as possible, e.g. by setting the accounts of underage users to be private-by-default or by minimizing the amount of data collected.
Profiling	The practice of using an individual's personal data to infer, predict or analyse characteristics about that person, e.g. their likes, dislikes, preferences, views, opinions or behaviour, to recommend content, products or services based on the person's data profile.
Safety-by-design	The practice of designing online services with the aim of ensuring users' safety as much as possible, e.g. by default safe settings for accounts of underage users or by preventing adults from contacting underage users.
Targeted advertising	The practice of showing particular adverts to users based on data collected about them, e.g. their online activity, purchases, location, gender, age, preferences, etc.
Virtual and augmented reality	Virtual reality: The computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special digital equipment, such as a helmet with a screen inside or gloves fitted with sensors. Augmented reality: A simulation of the physical world with altered characteristics or supplemented items, usually experienced through a screen to enable the overlay of virtual objects over a live image or video of reality.

About 5Rights Foundation

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world. While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities.

Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children, so that digital products and services can impact positively on the lived experiences of young people.

Find out more
Visit www.5Rightsfoundation.com or contact info@5rightsfoundation.com

Building the digital world that young people deserve.