Submission on the Draft General Comment: Children's rights in the digital environment

defenddigitalme advocates for children's digital rights in the education sector in England and beyond. Funded by the Joseph Rowntree Reform Trust.

defenddigitalme.org/the-state-of-data-2020/

III. General principles

A. Right to non-discrimination

1. **Add in paragraph (11)** …"unfairly obtained information. **Children may be unaware of discrimination resulting from not using a digital service or exclusion from the data cohort used to train a product or to determine differential treatment, such as consumer pricing. Such discrimination should be perceived similarly to that which that can be positively seen."**

B. Best interests of the child

2. **Paragraph (14)** …"children's rights in such environments, **by carrying out a Child Rights Impact Assessment (CRIA),** contrasted with the interests and rights of others, and shall apply […] criteria have been applied **through publication of the CRIA."**

D. Right to be heard

3. **Paragraph (19)** …"applying appropriate safeguards and **inclusive design standards,** and give their views due consideration when developing their services, **in particular of State services."**

IV. Evolving capacities

4. **Add after paragraph (22)**:

   "**States should ensure that due consideration is given to the prior right of parents to choose the kind of education that shall be given to their children in accordance with Article 26 of the UNDHR[1] when offering education services in the digital environment."**

V. General measures

5. **Paragraph (23)** …"consult with children, their parents and caregivers, **as well as representative bodies in civil society."**

B. Comprehensive policy and strategy

6. **Paragraph (26)** In this broad statement there should be no narrowing of what is considered important in measures that protect children. Instead of limiting these through specificity, since even a long list will never be comprehensive, and because "including from online sexual abuse and exploitation," is included in the document in several other places, edit to read:

   …"Such measures should protect children, and provide remedy and support for child victims and measures to meet the needs of children in disadvantaged or vulnerable situations, including resource materials translated into relevant minority languages."

7. **Paragraph (27)** "operation of **safe, lawful, transparent, and** effective **online child protection** and safeguarding policies …"

[1] UNDHR Article 26 https://www.un.org/en/universal-declaration-human-rights/

C. Coordination

8. **Paragraph (28)** "…government body, **placed on a statutory footing,** that is mandated…"

D. Allocation of resources

9. Add after paragraph (30)

   "**Where State services for children are supported in the digital environment by resources provided for by parents, States must ensure no discrimination results from those who can pay for them and those who cannot, to ensure equity in access to services, such as in the provision of education or access to child welfare support through a digital-first application policy."**

E. Data collection and research

10. **Paragraph (31) "…**production of **necessary and proportionate** robust, comprehensive data that is adequately resourced. Such data and research, including conducted with and by children, should **have appropriate ethical oversight,** inform regulation, policy and practice and should be in the public domain, **while also meeting all necessary and statutory safeguards for privacy and data protection."**

G. Dissemination…

11. **Paragraph (34)** "educational" rather than *learning* settings.

J. Commercial…

12. Add after **Paragraph (43)**

    "Where an imbalance of power exists between the State and parent or child, advertising in the digital provision of state services, such as education, should be prohibited as best practice, since consent cannot be freely given and is therefore invalid."

V. General measures. F. Independent monitoring

13. States should support mechanisms to monitor algorithmic discrimination in public services, such as adopted in The Netherlands, Finland[2] and New Zealand[3]:

    Add after **paragraph (32) "States should ensure that the use of any automated and algorithmic decision making in the delivery of state services is recorded and published in a national transparency register, and that they give due consideration to the full range of children's rights in the development of standards and Codes of Practice regarding such adoption and use."**

VI. Civil rights

---

[2] Johnson, K (VentureBeat) 2020 | Amsterdam and Helsinki launch algorithm registries to bring transparency to public deployments of AI https://venturebeat.com/2020/09/28/amsterdam-and-helsinki-launch-algorithm-registries-to-bring-transparency-to-public-deployments-of-ai/

[3] Graham-McLay, C. (The Guardian) 2020 | New Zealand claims world first in setting standards for government use of algorithms https://www.theguardian.com/world/2020/jul/28/new-zealand-claims-world-first-in-setting-standards-for-government-use-of-algorithms

A. Access to information

Text should avoid the age-appropriate label, but focus on a child's evolving capacity. Age gateways may serve commercial providers well, but encourage a gap in parental oversight 13+, excessive data processing and exploitation.[4] We suggest wording should always ensure that age-verification (AV) systems are not encouraged, or permitted, to collect additional data for AV or use it for other purposes.

14. **Add to Paragraph (56)** …"principle**s** of data minimisation, **necessity, and purpose limitation."**

We would welcome strengthened safeguards on filtering and monitoring. State and commercial (ab)use of such technology infringes rights, is routine, and its efficacy is disputed.

Brennan Centre research 2013-18[5] on U.S. schools and social media monitoring software, highlighted: *"Aside from anecdotes promoted by the companies that sell this software, there is no proof that these surveillance tools work [compared with other practices]. But there are plenty of risks. In any context, social media is ripe for misinterpretation[6] and misuse."*

2013 Report from the Special Rapporteur[7] noted, "*States can use such technologies to detect the use of specific words and phrases, in order to censor or regulate their use, or identify the individuals using them. […] Internet filtering reportedly enables the censorship of website content and communications and facilitates the surveillance of human rights defenders and activists*."

2001 UNCRC GC/1 on the aims of education[8] was clear, *"Children do not lose their human rights by virtue of passing through the school gates."* The Committee should note filtering and monitoring 'in the school digital environment', goes beyond school hours and on school grounds.[9]

School safeguarding systems monitor children's activity, 24/7, 365 days a year. Many read passwords[10] and sensitive content. Breaking end-to-end encryption is routine and results in interferences with children's privacy. Our U.K. analysis of fifteen providers revealed unlawful practice and risks from sensitive data transfers abroad. Explicit, sensitive personal data is even exploited by one company for its own marketing.[11] Such services can result in over-blocking and definitions of terrorist content (against which terms children are profiled) are over broad. There is scope creep from picking out content, towards picking out children, under vague definitions of 'extremism'.[12] Providers do not offer independent evidence of efficacy or transparency statistics.

---

[4] Persson, J. (2017) Google Family Link for u-13s: children's privacy friend or faux? https://jenpersson.com/google-family-link/ "*In return, Google gets access to a valuable data set – a parent-child relationship with credit data attached. Yet Google can't guarantee additional safeguarding, privacy, or benefits for the child while using it."*

[5] Patel, F. (2019) The Brennan Center https://www.brennancenter.org/our-work/research-reports/school-surveillance-zone School districts are spending more on social media monitoring technology, but there is little evidence it is keeping students safer.

[6] Duarte, N. (2017) Center for Democracy and Technology *Mixed Messages? The Limits of Automated Social Media Content Analysis* https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/

[7] 2013 Report of the Special Rapporteur (right to freedom of opinion and expression) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (Section D, para 45)

[8] General Comment No. 1: Aims of Education (article 29) (para 8) https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/a)GeneralCommentNo1TheAimsofEducation(article29)(2001).aspx

[9] CEO, eSafe, Parliamentary Committee on Children and the Internet (2016) "*… the behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon, clearly; it is 24/7 and it is every day of the year. Lots of our incidents are escalated through activity on evenings, weekends and school holidays."* http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html

[10] Smoothwall https://kb.smoothwall.com/hc/en-us/articles/360002135724-Frequently-Asked-Questions-FAQs- "*Monitor Managed Service captures everything that a user types, which can even include items they subsequently delete. Because it works on keystrokes, … it doesn't matter what program the user is typing in, or how it's encrypted."*

[11] eSafe marketing (2020) https://twitter.com/TheABB/status/1259142055126806529?s=20 *"… student had been writing an emotionally charged letter to her Mum using Microsoft Word, in which she revealed she'd been raped. Despite the device used being offline, eSafe picked this up…"*

[12] UN human rights experts concern on EU counter-terrorism proposal (2018) https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24013&LangID=E "*We recognise the need to prevent the dissemination of terrorist content online,*" the experts said. *"However, we have serious concerns that the Proposal's overly broad definition of what constitutes 'terrorist content' could include legitimate forms of content."*

15. **Add to Paragraph (57)** …"balance protection against children's rights, **and uphold** their rights **to access information**, freedom of expression and privacy. **Such controls should focus on content, not child identification or the profiling of individuals and their activity. Such controls must permit access to counselling services and promote children's confidentiality in their use. Companies offering such controls publish transparency statistics on which content is filtered and blocked, what has been monitored, and their error rates."**

E. Privacy

16. We welcome **paragraph (72**) on "privacy-by design, such as end-to-end encryption, in services that impact children." We encourage the Committee to resist attempts to weaken protections on end-to-end encryption, necessary for children's safe communications / financial transactions. One cannot weaken encryption to only give 'good guys' access to a secure digital environment.

    "*On 27 July, the European Commission published a Communication on an EU strategy for a more effective fight against child sexual abuse material (CSAM). […] This should be good news for the millions of people using these services who will see better protection of online communications but it has been perceived as a threat*."[13] (EDRi)

    The changes do not affect the Law Enforcement Directive[14] where applicable to data processing in the pursuit of crime, including CSAM, or the application of the GDPR[15] or Convention 108+. The Committee should be alert to the risk that child-rights messaging may be misappropriated by States seeking greater surveillance powers for other purposes, beyond the best interests of the child. We note the recent statement[16] from the Five Eyes[17] nations Australia, Canada, New Zealand, the United Kingdom, and United States, (plus India and Japan) on end-to-end encryption.

    The Special Rapporteur 2013 Report[18] on the right to freedom of opinion and expression, noted human rights breaches including, "*the Government of India is proposing to install a Centralized Monitoring System that will route all communications to the central Government, allowing security agencies to bypass interaction with the service provider. Such arrangements take communications surveillance out of the realm of judicial authorization and allow unregulated, secret surveillance, eliminating any transparency or accountability on the part of the State."*

17. **Paragraph (74)** the last line might conflict with data protection law, "*Where information is provided in one setting and can legitimately benefit the child by use in another setting, for example, school and tertiary education…*" Purpose limitation is key in the Convention 108+[19] and the GDPR, and the legitimate lawful basis would rarely be consent or appropriate to change to consent in an educational setting, since the child may be treated detrimentally if they or parents decline, and therefore consent is not freely given and invalid. Previous sentences adequately address this, and should not suggest weak exceptions.

---

[13] EDRi (2020) Is surveilling children really protecting them? https://edri.org/our-work/is-surveilling-children-really-protecting-them-our-concerns-on-the-interim-csam-regulation/ and multi-stakeholder civil society joint letter https://cdt.org/insights/cdt-joins-open-letter-on-civil-society-views-of-defending-privacy-while-preventing-criminal-acts/

[14] Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties… https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680

[15] European Data Protection Board (EDPB) view that an "encryption ban" would endanger compliance with the GDPR https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020-0061_mep_koernerencryption.pdf

[16] Statement from Five Eyes nations plus India and Japan (2020) https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety (this statement in the UK government website is filed under counter terrorism)

[17] Nyst, C. (2014) Global Information Society Watch | Unmasking the Five Eyes' global surveillance practices https://www.giswatch.org/en/communications-surveillance/unmasking-five-eyes-global-surveillance-practices#sdfootnote13anc

[18] 2013 Special Rapporteur report on the promotion and protection of the right to freedom of opinion and expression http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf *"the right to private correspondence gives rise to a comprehensive obligation of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without the interference or inspection by State organs or by third parties."*

[19] CoE Guidelines on data protection in educational settings (forthcoming) https://www.coe.int/en/web/data-protection/education-settings

Delete from (74) "Where information is provided in one setting … as appropriate."

18. We welcome in **para (75)** "includes public settings …" **and suggest it is strengthened** to better protect children in the public space from sensors they cannot see.[20]

    Add between (75) and (76), with reference from CCPR/C/GC/16 para. 78

    "**Providers of "smart" services in the public space must respect all children's rights and in accordance with domestic and international data processing law. Ensuring that the best interests of the child are a primary consideration in business-related legislation, policy development and delivery at all levels of government and commercial endeavours in the public space, requires child-rights impact assessment and ongoing monitoring and evaluation. Authorities should publish their intentions to adopt new measures that will result in children's data processing, maintain a public register of such measures, and publish regular monitoring reports."**

19. We welcome in **paragraph (78)** "*…such practices can be important to protect children's privacy*," **and suggest it is strengthened,** emphasising why young people want anonymity e.g on social media.[21]

    "Many children use avatars or names that protect their identity. Such practices can be important to protect children's privacy **and promote their full and free development and human flourishing**."

VII. Violence

20. **Paragraph (87).** It is unwise to conflate illegal content (CSAM) and what may be legal (bullying) in the role of business and without definitions, since the obligations and enforcement mechanisms are very different. Simplify to: **"States should ensure that business enterprises meet their responsibility to effectively protect children from all forms of violence in the digital environment."**

VIII. Family environment

21. **Paragraph (95).** This might be interpreted as a duty to examine parents to determine if they are "fully conversant." **Needs clarification.**

IX. Disabilities

22. **We welcome paragraph (98)** regarding online tools in education: "…ensure that technologies are designed for universal accessibility so that they can be used by all children without exception."

X. Basic…

23. **Paragraph 105.** Review for an error, and contradiction between paragraphs 105 "*States **should regulate targeted or age-inappropriate advertising**, marketing or service **designed to prevent** children's exposure to the promotion of unhealthy food and beverages,…*" and paragraph (42) "***States should prohibit by law the targeting of children of any age for commercial purposes** on the basis of a digital record …"*

---

[20] O'Flynn, S. (2019) *Protecting children's data privacy in the smart city:* The pattern of inattention should make us wary of granting Sidewalk Toronto access to resident and public data without a very clear understanding of what is tracked, archived, analyzed and shared.

[21] Film by the Warren Youth Group https://www.youtube.com/watch?v=FmVZE-Y4LNE *You are what you share*, includes (01:15) comments from young people on choosing "how you want to be represented"

As written, paragraph 105 suggests States should **not** regulate promotion and would **encourage** advertising of unhealthy or harmful products**.** We suggest this may be unintentional, and should say the opposite.

Making both consistent based on paragraph 42, might suggest re-writing 105 to read, "States should **prohibit by law** targeted or age-inappropriate advertising, marketing or services **designed to promote children's exposure to** unhealthy food and beverages, alcohol, drugs, …"

XI. Education…

24. **Paragraph 112** add "**advertising**" since this might not be considered 'commercial exploitation' but is widespread [22] "…of their personal data, **advertising,** commercial exploitation…"

XII. Special protection…

25. **Paragraph (122)** Add understanding that children's digital activity may generate information that becomes business intelligence and is in effect, child labour, used by companies[23] to enhance and develop products and markets through meta data exploitation.[24]

"…other forms of exploitation. **The Committee notes that where children's digital activity is surveilled and used to create behavioural data from browser fingerprinting (also known as device fingerprinting), this may create information used for product enhancement and development, and as such is economic exploitation.** States should…."

XIII. International…

26. **Paragraph (127)** add final word "…**environment.**"

---

[22] State of Data 2020 report defenddigitalme.org/the-state-of-data-2020/

[23] Ferreira, J. (2012) CEO, Knewton | 01:33 'Knewton gets 5-10 million actionable data points per student per day' https://www.youtube.com/watch?v=Lr7Z7ysDluQ 02:51 "If you do ten minutes of work in Google, you produce data points **for Google**, but if you do ten minutes of work **for Knewton** you cascade out lots and lots of other data"

[24] Briz N. (2018) Mozilla | What is Browser Fingerprinting? https://blog.mozilla.org/internetcitizen/2018/07/26/this-is-your-digital-fingerprint/