5RIGHTS FOUNDATION

Online Safety Bill briefing

March 2022

5Rights welcomes the publication of the Online Safety Bill and the opportunity it presents to deliver systemic change on behalf of UK children. We are disappointed that the government has accepted fewer than half of the Joint Committee's recommendations and that the Bill does not reflect the calls of the children's sector to provide children with holistic and binding protections.

From social media feeds recommending self-harm or disordered eating content, the metaverse enabling direct contact between children and adults they do not know[1] to games littered with gambling style features and persuasive design techniques, children are routinely exposed to a huge range of harms online. The Online Safety Bill presents a singular opportunity to change that and give children the protections they need.

This document details six ways in which the Bill must be amended if it is to deliver on the government's promise of protecting children and making the UK the "safest place in the world to be online."

1. The Bill must protect children's rights to participation and freedom of expression

As well as offering children protection online, the Bill must uphold children's rights to participation and to free expression as set out in the United Nations Convention on the Rights of the Child (UNCRC). **The government's assertion that the Bill "already reflects the principles of the UN Convention" is not reflected in the text itself.**[2] To ensure children are not frozen out of spaces they have a right to access, or have their voices silenced, the UNCRC must be cited on the face of the Bill, and services must prioritise the best interests of the child.

Children's participation and speech rights and their rights to protection are not mutually exclusive. The Bill must not force services to choose between them. To ensure their best interests are always prioritised, the Online Safety Bill must cite the UNCRC on the face of the Bill.

2. The Bill must apply to all services *likely to be accessed* by children

Children require protection wherever they are online. The Age Appropriate Design Code[3] has set the bar for child protection, requiring all services likely to be accessed by children to provide high levels of data protection and privacy. But the Online Safety Bill

---

[1] Metaverse app allows kids into virtual strip clubs, BBC, 22nd February 2022

[2] "The Bill already reflects the principles of the UN Convention on the Rights of the Child General Comment No.25 on children's rights in the digital environment." Government Response to the Report of the Joint Committee on the Draft Online Safety Bill, March 2022, p. 35.

[3] Age Appropriate Design Code, Information Commissioner's Office

will regulate only user-to-user and search services, and will not apply to all services who fall in scope of the Age Appropriate Design Code. **This will create a patchwork of regulation, risking uncertainty for companies and the prospect of decades of legal battles.** Regulatory alignment aids compliance and will simplify enforcement for Ofcom and the ICO.

Parents have the reasonable expectation that children will be protected wherever they are online under the new regime. They cannot be expected to be aware of exemptions or distinctions between categories of service: they simply want their children to be protected and their rights upheld wherever they are. The following services will remain out of scope of the new regime unless the scope is extended to all services likely to be accessed by children:

- **Harmful blogs that promote life-threatening behaviours, such as pro-anorexia sites, with provider-generated (rather than user-generated) content**
- Some of the most popular games among children that do not feature user-generated content but are linked to increased gambling addiction among children.[4] Some families have lost thousands of pounds to such games.[5]
- Services with user-generated content that is harmful but does not affect an "appreciable number of children", risking dozens, hundreds or even thousands of children falling unprotected.

The Bill must be amended to cover all services *likely to be accessed* by children, on the same basis as the Age Appropriate Design Code.

3. The Bill must ensure that Codes of Practice relating to child safety duties are mandatory and binding

The Bill instructs Ofcom to produce separate codes of practice for child online safety and countering child sexual exploitation and abuse, but neither have statutory status, and will provide only "recommended guidance" for regulated companies.

This is inadequate. **It is vital the Bill is unequivocal about the kinds of risks children are exposed to online as well as the steps that Ofcom would require companies to take to address them.** The risks are not confined to age-inappropriate content, but in greatest part are a result of the features and functionalities such as algorithms and recommendation systems that create risk and amplify harm.[6] **Harms to children should be defined on the face of the Bill, not left to secondary legislation, and the steps to eliminate, mitigate and manage the risks of those harms arising must be outcome-based and binding.** Setting out clear expectations will help services implement safety by design solutions, and prevent 'tick-box' compliance or the widespread introduction of heavy-handed parental controls that may be unsuitable for older children.

[4] Video game loot boxes linked to problem gambling, study shows, the Guardian, 2nd April 2021

[5] Parents including doctor who had to sell his car reveal how they have lost a fortune to tech firms 'tricking' children into buying upgrades for free games, the Daily Mail, 14th July 2021

[6] Risky by Design, 5Rights Foundation

The Code of Practice for Child Online Safety must cover each of the 4 Cs of online risk,[7] and consider: safety by design, published terms, moderation, reporting and redress, as well as educational initiatives and digital and data literacy taught in schools (or delivered by other means).

Codes for child online safety and CSEA must be binding and apply to all services likely to be accessed by children.

4. The Bill must establish standards for privacy-preserving age assurance

The protections to children envisaged by the Bill will require some services, depending on the level of risk they carry, to have age assurance in place to identify users under the age of 18. The revised Bill contains a welcome recognition that these age assurance systems must not be implemented at the cost of user privacy, but the Bill itself does not set out how this is to be achieved. Instead, the government has indicated it will rely on companies to adhere to voluntary industry standards. This is not adequate to assure levels of privacy, inclusivity and security needed to make age assurance effective.

Age assurance must be proportionate, rights-respecting, privacy-preserving and effective. **Reluctance from service providers to implement age assurance is not due to a lack of technical solutions: there are many viable methods, from the use of age tokens to biometric analysis.[8] Rather, the reluctance stems from an unwillingness to shoulder the responsibilities that accompany the knowledge that the end user is a child.** The Bill should set the expectations, not the technical standards, to ensure that the innovation and creativity of the sector will meet, however reluctantly, the bar that has been set.

An age assurance code of practice must be fast-tracked and backed up by binding standards that establish rules of the road. Without fast-tracked age assurance, children will have to wait for another three years, during which they will inevitably endure otherwise avoidable harm.

The Bill must task Ofcom with creating a code of practice for age assurance with binding standards of efficacy, security and privacy. This work should begin immediately so that it is ready as the Bill receives Royal Assent.

---

[7] The 4Cs of online risk are: content risks (exposure to harmful material); contact risks (exposure to activity with a malign actor); conduct risks (involvement in an exchange as either a victim or perpetrator); and contract risks, sometimes called commercial risks (exposure to inappropriate commercial contractual relationships or pressures). The 4Cs: Classifying Online Risk to Children, S. Livingstone and M. Stoilova

[8] Age tokens contain only information relating to the specific age or age range of a user, biometric data such as height, gait, voice, facial features, keystroke dynamics or finger prints can be used to estimate age, and cross-account authentication refers to the use of an existing account to gain access to a new product or service. For more information on the range of available age assurance solutions, see *But how do they know it is a child?*, 5Rights Foundation, October 2021

5. The Bill must give bereaved parents access to data in cases where a child has died

The government has stated that the needs of bereaved parents are "outside the scope of this Bill",[9] and in spite of considerable evidence to the contrary, has asserted that coroners already have the necessary powers to require access to data following the death of a child.[10]

This is a truly callous response to the plight of families looking for and routinely denied answers to the circumstances surrounding a child's death. More profoundly, **it fails to acknowledge that the absence of oversight in cases of death allows the companies to continue to algorithmically recommend the same material to other children – potentially contributing to further tragedy.**

Molly Russell was 14 years old when she took her own life.[11] Her father Ian has spoken about how the content she saw in the months leading up to her death escalated and encouraged her depression.[12] Frankie Thomas's family struggled to get answers from the service they knew Frankie spent time using before her suicide, and they are still denied access to what Frankie was seeing at the time of her death.[13] Her mother has said Instagram had treated the family's request for details of their daughter's account as though they had "lost some property." After months of receiving no response, only automated messages, Instagram finally told Frankie's parents they could only provide them with "basic subscriber information" about Frankie's account. Even that information would require them to obtain a court order. Mr Thomas compared the process of retrieving information to a "war of attrition where they think 'if we say no enough times then the bereaved parents will just shut up, go away and stop pestering us'."[14]

Most children die without a will and their parents are the next of kin. They are given the contents of the school locker, they have access to the contents of their bedrooms: to be locked out of their digital lives, including their photographs and their posts, leaves them bereft. To be prevented from seeing the material that may have contributed to their death is simply inhuman. While the privacy of other users is a factor to consider, there is simply no excuse to deny the coroner, regulator and in most cases parents, access to a child's digital life.

---

[9] "Disclosure of data relating to a deceased person falls outside the scope of this Bill." Government Response to the Report of the Joint Committee on the Draft Online Safety Bill, March 2022, p. 67.

[10] "Coroners already have statutory powers to require evidence to be given or documents to be produced for the purpose of their inquests (which would include relevant digital data following the death of a child)." Government Response to the Report of the Joint Committee on the Draft Online Safety Bill, March 2022, p. 68.

[11] Molly Russell: Social media users 'at risk' over self-harm inquest delay, BBC News, 8th February 2021

[12] Instagram 'helped kill my daughter', BBC News, 22nd January 2019

[13] These tech giants led Frankie to kill herself. So why won't they talk to me?, Judy Thomas, The Times, 27th March 2022

[14] Instagram shuts parents out of account of daughter who killed herself after viewing self-harm sites, The Telegraph, December 2021

The Bill must be amended to create a fair process for bereaved parents, the regulator and coroners to access children's data in a timely way, to protect against further harm and to offer closure to families.

6. The Bill must fast-track protections for children

The reliance on secondary legislation to clarify some of the most important aspects of the new regime and the time it will take for Ofcom to draft multiple codes of practice is likely to mean children will be waiting another three years before they receive the safeguards they have been promised.

The government should fast-track, at a minimum, children's safety codes of practice, risk assessments and minimum standards for privacy-preserving age assurance. Crucially, harms to children should be set out in the primary legislation. There is already an extensive evidence base from which the typology and nature of risks to children online can be defined under the legislation. Below are examples from five major pieces of research from the last five years that evidence the harms children face online:

- Pathways, a ground-breaking research project, highlights how design decisions pave the way for harm to children. It shows how tech companies are targeting children with advertising while recommending those same children self-harm, extreme diet and pro-suicide material.[15]
- Risky by Design illustrates how common design features pose risks to young people in the digital world.[16]
- The Internet Watch Foundation reports that there has been an "exponential increase" in self-generated child sexual abuse material, often created using livestreaming and video-sharing features common to online platforms and then shared across those same services.[17]
- Disrupted Childhood, a 5Rights report, considers the impact of persuasive design and the features of online services that create an ecosystem of distraction, competition and invasion and cause anxiety, sleeplessness and negative impacts on the health, education and social life of children.[18]
- The British Board of Film Classification has shown how almost half of children (47%) have been exposed to disturbing content online, and one in seven (13%) see such content every day.[19]

[15] Pathways: How digital design puts children at risk, 5Rights Foundation, July 2021

[16] Risky by Design, 5Rights Foundation

[17] Self-generated child sexual abuse, Internet Watch Foundation

[18] Disrupted Childhood: The Cost of Persuasive Design, 5Rights Foundation, June 2018

[19] Half of children and teens exposed to harmful online content while in lockdown, British Board of Film Classification, 4th May 2020

- Ofcom's own research from 2020 revealed 81% of 12-15 year olds have had a potential harmful experience online.[20]

The harms children face evolve with every new product and service. Most are not the result of bad actors or those with malicious intent but a result of the design and functionalities of services themselves, and a collective failure to commit to safety by design. There are legitimate, and frustrating, reasons that the Online Safety Bill has been so delayed, but government must act now and make certain that yet another generation of children do not come to such avoidable harm.

Harms to children should be on the face of the Bill, and Ofcom should be tasked with drafting children's codes of practice and minimum standards for age assurance now, so that they can be introduced as soon as the Bill receives Royal Assent.

Conclusion

The government's approach to the Bill has made it complex and content-focused, when what is required are standards of product safety that can be enforced against agreed criteria. The Bill has also ignored existing research and evidence, and deferred many of the key aspects of the new regime to Ofcom to build out. This will undoubtedly engender costly and lengthy periods of consultation. The sector is innovative and creative, and while it has shown reluctance to prioritise children's safety, the changes made in compliance with the UK Age Appropriate Design Code show that when required, they really can design with safety in mind. The Bill should take this safety by design approach and it should act with the speed that is necessary. Each day that they fail to do so, children are coming to very real harm.

[20] Online Nation Report 2020, Ofcom, p. 5