DCMS Sub-Committee Inquiry

Online Safety and Online Harms

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.

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.

5Rights Foundation speaks specifically on behalf of and is informed by the views of young people. Therefore, our comments reflect, and are restricted to, the experiences of young people under the age of 18. However, we recognise that many of our views and recommendations are relevant to other user groups and we welcome any efforts that government makes to make the digital world more equitable for all user groups, particularly the vulnerable.

Responses to Consultation Questions

1. How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

The change in language from 'online harms' to 'online safety' reflects the journey the Bill has taken from its initial conception in 2017 as a green paper to the draft Act published in May 2021. It is a welcome recognition of the limitations of an approach which focuses on responding to harm after it has occurred, and of the need to make online services safe by design. To be effective, the legislation must be accompanied by enforceable, clear, systemic and mandatory standards of safety by design that will ensure digital products and services meet the government's stated policy objectives.

5Rights recommends:

A) The legislative requirement for providers to make their services safer by design must be on the face of the Bill if the safety objectives are to be achieved. Ofcom must be charged with producing mandatory and enforceable standards for safety by design contained in statutory Codes of Practice.

2. Is it necessary to have an explicit definition and process for determining harm to children and adults in the Online Safety Bill, and what should it be?

Yes, it is necessary to have an explicit definition and process for determining harm to children and adults in the Bill.

Definition of harm

The draft Bill has been rebadged since the government published its full response to the white paper in December, as legislation designed to address harmful ***content***. This misses a range of potential harms that result from contact, conduct and contract risks (known as the 4 Cs).

The focus on content opens up the government to accusations of undermining freedom of expression, rather than taking the more neutral and holistic approach to tackle risk at a systemic level. It also puts an emphasis on allowing harm to happen and responding to it, rather than addressing the systems and design features of the digital world that encourage the creation and amplification of harmful behaviour, activity and material.

Harmful content is given the meaning of content that has a significant adverse physical or psychological impact (clause 45, paragraph 3). This does not capture material or behaviour which alone may not cause immediate harm, but can in combination and over time have a severe impact on a child's safety and wellbeing.

Existing regulatory definitions of harm should be built upon in the Bill, particularly the definition of harm to children included in the Communications Act 2003[1] and Ofcom's video-sharing platform guidance[2] as anything which "might impair the physical, mental or moral development of persons under the age 18."

5Rights recommends:

B) The language of 'content **and activity**', from the Full Government Response, should be reinstated whenever the Bill refers to the obligations on regulated services to address harmful content. All references to harmful content, and the meaning of content that is harmful to children in clause 45, should be amended to refer to harmful content "and activity", or the definition of harmful content should be amended to be simply a definition of "harm".

Risks to children vs risk to adults

The references to "children in different age groups" in the safety duties relating to children (clauses 10 and 22) are a welcome recognition that children of different ages have different needs and vulnerabilities, and experience different types and levels of risk. But this is not supported by a clear commitment to set out the standards of behaviour and design expected of service providers.

Recent changes announced by several global companies as they seek to meet the mandatory requirements of the Age Appropriate Design Code (AADC)[3] have shown just how powerful a statutory code of practice can be. In the case of the AADC, the 15 standards have led to companies assessing their services and introducing design changes as significant as stopping targeted advertising to children, introducing high privacy default settings, turning off location tracking and prohibiting direct messaging between children and unknown adults. An analogous code of practice for children's online safety to accompany the Online Safety Bill would do for children's safety what the AADC has done for their privacy.

5Rights recommends:

C) Ofcom should be charged with creating a mandatory Child Online Safety Code of Practice that sets out the typology of risk to children (using the 4 Cs risk framework), recognising the changing nature of risks to children of different ages. This code should build on the extensive knowledge that has been built up in the third sector, and be compatible with the provisions of the AADC.

Determining risk and harm

[1] Communications Act 2003
[2] Guidance for providers on measures to protect users from harmful material, Ofcom.
[3] Age appropriate design: a code of practice for online services.

Services likely to be accessed by children have a duty to undertake a children's risk assessment, keep it up to date, and update it before making any significant changes to the service, but they will not be required to publish their risk assessment (Clause 7) (unlike Category 1 services, who are required to publish their freedom of expression and privacy impact assessments). Providers can be punished for failing to undertake or hand over their risk assessment to the regulator, but there is no similar accountability for the scope, quality or speed of mitigation for the risks the assessment reveals. Without minimum standards for the risk assessment process, the quality and efficacy of the assessments will not offer certainty across the sector. Greater clarity about the duty to prevent and mitigate risk, rather than simply report it, is needed if the risk assessment is to remain the prime mechanisms for risk reduction.

Throughout the Bill, there are concessions for small businesses, designed to reduce the regulatory burden. For example, in determining whether mitigation measures are 'proportionate', the size and capacity of a provider will be considered (Clause 10). But small does not necessarily mean safe and often small services have insufficient (or no) safety settings, moderation or reporting processes in place. Small companies should be given the support they need to comply with regulation, not permission to harm.

> The video-sharing platform Clapper has under 500,000 downloads on the Google Play store. Despite a minimum user age of 17, the service's ineffective age assurance means a child can log into Clapper via their Google account, even if they are underage. The service is known to harbour misinformation and its terms of service explicitly state that it "cannot ensure the prompt removal of objectionable material as it is transmitted or after it has been posted."[4]

Ofcom is charged with carrying out a sector risk assessment to identify, assess and understand the risks of harm to individuals presented by regulated services, and developing risk profiles for different kinds of services (Clause 61). Rather than an exhaustive list of harms, which is unlikely to capture all emerging risks, Ofcom should use the 4 Cs risk framework to identify different types of risk to children, providing illustrative examples for each category of risk. Ofcom's risk profiles, along with an ***overarching duty of care*** (not currently set out in the Bill) to protect users and mandatory, ongoing risk assessment requirements, will futureproof the Bill and ensure it protects children against emerging and future risks.

5Rights recommends:

D) The Bill must require services likely to be accessed by or impact children to assess risks against the 4 Cs risk framework, in accordance with minimum standards for the risk assessment process set by Ofcom, and to publish their risk assessments.

[4] See: https://newsclapper.com/terms

E) The online safety objectives (clause 30) and duties for regulated services, must set a high bar of safety requirements for all providers, regardless of size. Small companies must be given more support to comply with the regime, not permission to harm.

3. Does the draft Bill focus enough on the ways tech companies could be encouraged to consider safety and/or the risk of harm in platform design and the systems and processes that they put in place?

No (see recommendation B).

The problems children face from the digital world are systemic. They are not restricted to technical bugs, bad actors, or individual pieces of content, but are also present in the features and architecture of the products and services that make up the world they inhabit.

There are references to "systems and processes" throughout the Bill, and as part of the risk assessment requirements, services will need to consider how "the design and operation of services (including the business model, governance and other systems and processes) may reduce or increase the risks identified." This is welcome, but critically, the duty for services to use proportionate systems and processes to minimise risk is included only in relation to addressing harmful content, which, as set out in our response to question one, must be redrafted as harmful content and activity, or simply as harm.

Although DCMS have now published their Safety by Design guidance, a *mandatory* safety by design framework set out in a statutory Code of Practice is needed to usher in a new world of digital design, set out clear expectations and ensure that services, both big and small, understand that some design choices are simply not appropriate in relation to children.

5Rights recommends

F) Safety by design must underpin the duties and requirements for products and services likely to be accessed by or impact children, to effectively remove, mitigate and manage all risks, not only content risks (see recommendation B).

G) Compliance with the safety by design requirements should be assessed against enforceable minimum standards. These should include minimum standards for the child risk assessment process (including the definition of risk and harm), as well as published terms, age assurance, and moderation, reporting and redress systems.

4. What are the key omissions to the draft Bill, such as a general safety duty or powers to deal with urgent security threats, and (how) could they be practically included without compromising rights such as freedom of expression?

Duty of care

The Bill contains a prescribed list of individual duties rather than an overarching, principle-based duty of care, with the potential for specific risks to be left unaddressed if they are not covered by one of the enumerated duties. Moreover, the list of duties is not as strong as the online safety objectives set out in clause 30. Specific duties can improve the safety of digital services and products, but this approach does not recognise the way risks are interconnected, cumulative and quick to evolve.

Having a single duty to meet the safety objectives would be a more straightforward, implementable and ultimately enforceable structure for the Bill. A duty of care would futureproof the Bill and ensure that the regulator is not always behind the curve as new technologies and products (and associated risks) emerge.

5Rights recommends:

H) The Bill should contain an overarching duty of care for regulated service providers to fulfil the safety objectives set out in Clause 30, which would also futureproof the legislation.

Exemptions and scope

Only services that are 'user-to-user' or 'search' services are in scope of the Bill. This will leave some services that carry significant risks to children out of scope, including app stores and some commercial pornography sites, where a lack of adequate age assurance and verification exposes children to inappropriate material and activity. Other services have been given specific exemptions, including services managed by education institutions and internal business services, which creates pockets of the digital world that have no responsibility for children's safety. Children have a right to protection wherever they are and all services likely to be accessed by or impact children should be regulated services, whatever their size, business model or nature, including services that may not fall under the definition of a user-to-user or search service. There should be no carve outs or concessions for smaller services but instead a proportionate enforcement regime, with smaller services given greater support to comply.

5Rights recommends:

I) All online services likely to be accessed by children must be in scope of the Bill and subject to an overarching duty of care, including those that do not fall under the definition of 'user-to-user' or 'search' services. Our proposed amendment to "meaning of regulated service" would bring all services that pose risks to children, including commercial pornography providers, in scope of the online safety regulation (see Annex A).

Advertising

The Bill is a historic opportunity to bring online advertising under a single regulatory regime, but as drafted most advertising remains out of scope. Paid-for-ads (where this is a contract between the provider and the advertiser) are given specific exemption, and

the statutory rules for paid-for advertising under the current VSP regulation[5] will be lost when the Online Safety Bill (which is to supersede the VSP regulations) comes into force, with children left exposed to ads containing financial scams and age-inappropriate products.

Over a three month period in 2020, the Advertising Standards Authority identified 159 age-restricted adverts which broke advertising rules by targeting their ads at services with high numbers of child users, including 70 different gambling ads and ten different alcohol ads.[6]

5Rights recommends:

J) The Bill offers the opportunity to put all online advertising regulation on a statutory footing, with proper enforcement powers to protect children from exposure to online advertising that has a detrimental effect on their physical, mental and moral wellbeing.

Financial and consumer harms

It was announced that the Bill will address some financial and consumer harms that are user generated (previously out of scope in the FGR) such as 'romance' scams' on dating apps and fake investment opportunities. These announcements are not reflected in the draft Bill. However the current scope and promised inclusions do not cover fraud via advertising, emails or cloned websites. If these types of consumer and financial harm are left out of scope, children remain at risk from online scams, gambling-style features and inappropriate commercial pressures that can lead to the accrual of debt, financial losses and service/contract lock-ins.

Gaming sites can put children at risk of financial harm through the presence of micro-transactions, loot boxes, and other in-app purchases. It is estimated between 25% and 40% of UK children who play online games have made a loot box purchase.[7] Children as young as four are spending money online and 5Rights research has shown that 80% of the top 50 'free' apps deemed suitable for children aged 5 and under on the Apple UK App store contain in-app purchases. Additionally, 1 in 10 children report making in-app purchases accidentally.[8]

[5] See: https://www.ofcom.org.uk/tv-radio-and-on-demand/information-for-industry/vsp-regulation
[6] See: https://www.asa.org.uk/news/protecting-children-online.html
[7] Lifting the Lid on Loot-Boxes, Chance-Based Purchases in Video Games and the Convergence of Gaming and Gambling, University of Plymouth, GambleAware and University of Wolverhampton, March 2021.
[8] Children as young as four are spending money online, The Telegraph, April 2021.

5Rights recommends:

K) The Bill should account for all known online harms to children, including financial and consumer harms. If these are not addressed by the Bill, the government should say how, when and through which regulatory lever they will be addressed.

Age Assurance

All regulated services will be required to assess whether their service is likely to be accessed by children. A service is to be treated as 'likely to be accessed by children' if it is possible for children to access the service, and that either a significant number of children are currently using the service, or it is likely to attract a significant number of child users. A service provider can only conclude that it is not possible for children to access their service if they have age assurance systems or processes in place which mean children are not normally able to gain access.

While these provisions are welcome, the Bill does not indicate the types of service or risk that require age assurance. Nor does it meet the promises made by former Culture Secretary, Rt. Hon. (Baroness) Nicky Morgan that the unrealised aims of part 3 of the Digital Economy Act 2017 (mandatory age verification on commercial pornography sites) would form part of the Bill, and that pornography will be put out of reach children through robust age assurance.[9]

Again, the Bill does not set out the standards to which the "systems or processes" preventing child access must adhere. Baroness Kidron (5Rights Chair) has introduced a Private Member's Bill[10] that would see Ofcom set out minimum standards for all age assurance systems, giving services confidence in the age of their users and ensuring that children are protected wherever they are online. The Age Assurance Minimum Standards Bill has been warmly welcomed by the industry, and closes a gap in the current legislative framework which urgently needs addressing. Moreover, the Bill could be implemented on a shorter timescale than the Online Safety Bill.

5Rights recommends:

L) The government should throw its support behind the Age Assurance Minimum Standards Bill so that the industry and Ofcom are prepared with effective and trusted age assurance to fulfil the current requirements of the AADC and those anticipated in the Online Safety Bill.

Codes of practice, minimum standards and enforcement

[9] Online Harms Statement, The Rt Hon Baroness Nicky Morgan, 16 October 2019. See: https://questions-statements.parliament.uk/written-statements/detail/2019-10-16/HCWS13

[10] Age Assurance (Minimum Standards) Bill [HL]. See: https://bills.parliament.uk/bills/2879

Ofcom has been tasked with preparing codes of practice, setting out "recommended steps" for services to take to comply with the duties in the Bill. The status of these codes of practice and the powers Ofcom will have to enforce them is ambiguous, with service providers given the option of proving they can comply with their relevant duties and the online safety objectives in other ways. It is unclear how the regulator can judge alternative approaches without referring to their own stated interpretation of what is necessary, which in turn means that providers should comply with the standards set out by the regulator. The possibility for providers to comply with the regime by "acting otherwise than by taking a step described in a code of practice" sets the scene for confusion and for companies with deep pockets to challenge decisions of the regulator.

The Bill contains duties relating to the systems and processes of services in scope, including enforcement of terms of service (Clauses 9 and 10), reporting and redress (Clauses 15 and 24) and age assurance (Clause 26). As written, however, the Bill does not require services to meet minimum standards in these areas. Without setting the bar, the Bill will not establish the necessary standards for safety that both users and providers of regulated services would like to see.

Regulated services must specify in the terms of service "how children are to be prevented from encountering content and how children in age groups will be protected from encountering it… and to ensure that the terms of service are clear and accessible, and applied consistently." If compliance with the regime is to be assessed against the provider's enforcement of their own terms and service, Ofcom must set out minimum standards for both the content and presentation of those terms of service.

Similarly, if a service provider can conclude (under Clause 26) that it is not possible for children to access a service or part of it, ("if there are systems or processed in place that children are not normally able to access the service or that part of it") then Ofcom must set out minimum standards for age assurance approaches to ensure the required level of security, privacy and accuracy in a service's age assurance methods.

5Rights recommends:

See recommendation G *(Compliance with the safety by design requirements should be assessed against enforceable minimum standards. These should include minimum standards for the child risk assessment process (including the definition of risk and harm), as well as published terms, age assurance, and moderation, reporting and redress systems.)*

Company director liability

The Bill reserves the right to issue criminal sanctions against individual company directors, but only when they have failed to comply with information requests from the regulator. The government would need to be persuaded to introduce director liability on the basis of significant failure across the market. It is highly improbable that the egregious and continued failure by one company would result in sanctions being brought in for all companies in scope. What is more, the government has delayed the introduction of the power until at least two years after the regulation comes into force,

following a review of the regulatory framework. This is not the swift, sharp, regulatory action needed when companies fail to engage. Without individual director liability, it is hard to see how the largest tech companies, whose enormous wealth and cash reserves can easily absorb even the heaviest fines, will be sufficiently incentivised to comply with a duty of care.

The Online Safety Bill should follow the precedent set by the Gambling Act 2005[11] and the Companies Act 2006[12] to hold individual responsible directors to account where they have failed to comply with the regulatory regime.

5Rights recommends:

M) Ofcom must be resourced to assess compliance against the regulation, and be given sufficient powers to effect the systems change needed across the sector, including the power to enforce financial and criminal sanctions against individual company directors for failures to fulfill the duty of care.

Algorithms (and automated decision-making)

The harmful nature of some content is supercharged by AI-driven models and algorithms of services that allow such content to reach large numbers of users. It is vital that the Bill addresses the ability of services to promote, recommend, spread, rank and prioritise harmful material through the use of AI-driven technologies and algorithms.[13]

The focus on content when algorithms are referenced in clause 7 on children's risk assessments (paragraph 9b iii) misses the central role that algorithms play in creating other risks, such as those associated with recommending friends/followers, groups to join, games to play or purchases to make. The online safety objective included in clause 30 to design and assess the service to protect users from harm, including through algorithms, functionalities, and other features relating to the operation of the service, is a better description of how services should address risks presented by algorithmic processes.

The Bill must require providers to ensure any AI-driven systems are fair to children, in particular that they observe their rights as set out in the UNCRC and general comment 25 on children's rights in relation to the digital environment[14], that they offer a high bar

[11] Part 5 and Schedule 7 of the Gambling Act 2005 concern operating licences issued by the Gambling Commission, including powers to revoke licenses and impose financial penalties.
[12] Companies Act 2006
[13] 5Rights has recently published its Pathways report, looking at the role of system design in children's online experiences. It reveals the way in which children are offered inappropriate content and contact even when they have been identified as children. Pathways offers irrefutable evidence that should spur the government to take a closer look at the role of algorithms in automating and promoting harmful outcomes for children.
[14] General comment No. 25 (2021) on children's rights in relation to the digital environment, United Nations Committee on the Rights of the Child.

of data protection as required by the Age Appropriate Design Code, and that they conform to UK laws concerning children. They must be required to provide information as requested by the regulator, such as information relating to the design, goals and outcomes of algorithms and allow access to personnel from product, governance, and marketing teams.

Under the information powers set out in clause 70, Ofcom can in theory request that providers provide information relating to the operation of AI-driven systems and algorithms in use on their services and what measures they have in place to mitigate these risks. What is missing in the Bill is the imperative for Ofcom to conduct these investigations on behalf of children. Children cannot be expected to understand or take action on automated decision making or algorithmic unfairness that has had a negative impact on them. Ofcom should have the duty as well as the expertise, resource, and processes in place to scrutinise the design goals, data inputs, model selection and outputs and outcomes of algorithms. Where there is evidence or an indication that such systems are discriminating against or systematically disadvantaging groups of people or violating their rights, Ofcom should set out a mandatory course of action for compliance.

5Rights recommends:

N) The clause 7 and 19 risk assessment duties must include requirements for companies to address both the intended and unintended consequences of their algorithms and automated-decision making processes and the full range of risks they create for children, not only content risks.

O) The Bill must give Ofcom a duty to investigate the automated decision-making systems and algorithms of regulated services that impact on children. Ofcom must provide statutory guidance in relation to these systems that impacts on children's rights and safety.

5. Are there any contested inclusions, tensions or contradictions in the draft Bill that need to be more carefully considered before the final Bill is put to Parliament?

The three counterbalancing 'protective' duties to address concerns about the impact of the Bill on freedom of speech were not included in the FGR. These are the duty about rights to freedom of expression and privacy (clause 12) and for Category 1 providers, duties in relation to content of democratic importance (clause 13) and protecting journalistic content (clause 14).

We welcome the inclusion of duties to protect freedom of expression and privacy, but they should be matched by acknowledgement of other rights, including freedom of thought, the right to access information and freedom of association. For example, Article 26 of the EU's proposed Digital Services Act (DSA) requires very large online

platforms to carry out an annual assessment of significant systemic risks arising from their services, including "any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child."[15]

The special provisions for journalistic content by recognised news publishers are also welcome (subject to agreed editorial control and a standards code) but the current definition of 'journalistic content' is so broad (news publisher or regulated content that is generated for the purposes of journalism and is UK-linked), it will undermine the very purpose of the duty – to protect news publisher content.

Similarly, the definition of 'content of democratic importance' (news publisher content or regulated content intended to contribute to democratic political debate in the UK) is so far-reaching, that it could be reasonably attached to any content. At best, this will create confusion for service providers about how to categorise user content. At worst, it will create significant loopholes that bad actors can easily exploit to challenge the removal of harmful content or activity.

Under Article 26 of the DSA, very large platforms must also consider the risk of "intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security." This is designed to prevent and mitigate the effects of activity that may undermine the democratic process or threaten national security. The Online Safety Bill could usefully borrow from this approach, which focuses on risk mitigation, rather than introducing additional duties that give private companies the power to arbitrate on the democratic importance of individual pieces of content.

Overall, these counterbalancing duties detract focus from the policy intent behind the Bill, which is to make the online world safer, and has had the reverse effect of potentially undermining free expression, opening up the regime to exploitation by those looking to spread hate online.

5Rights recommends:

P) The government should set out a clear hierarchy of intent in the Bill, stating the best interests of the child should be the primary consideration where tensions arise between freedom of expression and the safety of children.

[15] Article 26, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act), December 2020.

Q) The definition of journalistic content should be amended so that only recognised news publisher content (that is subject to editorial standards) is given additional protections under the regime.

R) The Bill should address threats to freedom of expression and the democratic process through the risk assessment duties, requiring services to have regard to the potential negative effects of their products and services.

Powers of the Secretary of State

In multiple places throughout the Bill, the Secretary of State is given the power to amend or repeal provisions (clause 3) and to direct Ofcom to modify its guidance (clause 33). This undermines the independence of the regulator, and its power to effectively enforce codes of practice and guidance.

5Rights recommends:

S) The powers of the Secretary of State as currently set out in the draft Bill must be tempered to ensure the independence of the regulator. Any proposals from the Secretary of State to amend or repeal provisions of the Bill should come before Parliament, and references to the power of the Secretary of State to direct Ofcom should be removed.

6. What are the lessons that the Government should learn when directly comparing the draft Bill to existing and proposed legislation around the world?

Age Appropriate Design Code

The UK's Age Appropriate Design Code is the first statutory code of practice for children's data protection in the world. It sets out standards to which companies must adhere when collecting, processing and sharing children's data, requiring a high level of privacy protection by default.
The Code requires services to appropriately safeguard children's personal data, ensuring children's profiles are 'private' by default, their locations are not tracked or made visible and their data is not shared with third parties or used to recommend content that is injurious to their wellbeing. It requires services to have risk-based age assurance and prohibits them from nudging children to lower their privacy settings, or to provide unnecessary personal data.

Services are changing how they process children's data and operate their services in direct response to the Code passing into law. Among a number of changes, TikTok[16] and Facebook[17] have changed their default privacy settings for users under the age of 16 and Google[18] and Facebook[19] have introduced limitations on targeted advertising to children. These changes will become widespread when the Code comes info full force in September 2021 and will impact directly on children's experience of the digital world.

Other jurisdictions are following the example of the UK and the Code to provide specific protections for children and their data. Most recently, the Irish Data Protection Commission produced the *Fundamentals for a Child-Oriented approach to Data Processing,*[20] to drive improvements in standards of data processing and enhance the level of protection afforded to children.

5Rights recommends:

See recommendation C *(Ofcom should be charged with creating a mandatory Child Online Safety Code of Practice that sets out the typology of risk to children (using the 4 Cs risk framework), recognising the changing nature of risks to children of different ages. This code should build on the extensive knowledge that has been built up in the third sector, and be compatible with the provisions of the AADC.)*

Australia e-Safety

The Office of the e-Safety Commissioner in Australia has produced a suite of Safety by Design tools[21] to support tech companies to ensure they are building safety into their products and services by default, and embedding safety into the culture, ethos, and operations of their businesses. By focusing on 'designing out' risk to reduce the likelihood of harm, safety by design tackles online safety at the systemic level and helps services to address risk 'upstream' through prevention and mitigation at the design stage, rather than responding to harm.

5Rights recommends:

T) The government should ensure its statutory safety by design regime includes and builds on the guidance from Australia's e-Safety Commissioner.

Ireland's Online Safety and Media Regulation Bill

[16] Strengthening privacy and safety for youth on TikTok
[17] Giving Young People a Safer, More Private Experience on Instagram
[18] Giving kids and teens a safer experience online
[19] Giving Young People a Safer, More Private Experience on Instagram
[20] Fundamentals for a Child-Oriented approach to Data Processing
[21] e-Safety Commissioner Safety by Design Assessment Tools.

Ireland's Online Safety and Media Regulation Bill has as one of its objectives "to protect the interests of children, taking into account the vulnerability of children to harmful content and undue commercial exploitation." The UK government should note this reference to the contractual risks and inappropriate commercial pressures that children face, and include in the Bill requirements to tackle these issues.

5Rights recommends:

U) The Online Safety Bill tackle harm at its root, by focusing on the operating practices, automated processes and design features of services, all optimised for commercial gain, that create risks for children.

UN General Comment 25

The UN Convention on the Rights of the Child is the single most important expression of children's rights and the needs of childhood and is the basis for much domestic legislation in relation to children around the world. The UN Committee on the Rights of the Child adopted general comment 25[22] on children's rights in relation to the digital environment in March 2021, setting out how legislators and regulators should implement and account for children's rights in the digital world and their obligation to ensure businesses respect the rights of children.

5Rights recommends:

V) As a signatory to the UN Convention on the Rights of the Child, the UK government is obliged to uphold children's rights and should cite general comment 25 on children's rights in relation to the digital environment on the face of the Bill.

OECD Recommendation on children in the digital environment

In May, the OECD published its Recommendation of the Council on Children in the Digital Environment.[23] In line with general comment 25, the recommendation calls for children's rights to be protected and respected in the digital environment, upholding the child's best interest as a primary consideration. It recommends a safety/privacy by design and default approach and calls on members, non-members and other actors to recognise all risk to children online, including content, contact, and conduct risks, as well as risks related to children as consumers, product safety, digital security, data protection and privacy.

The recommendation calls on Members to introduce legal measures and frameworks that are:

- fit for purpose, enforceable, and do not limit children's enjoyment of their rights;

[22] General comment No. 25 (2021) on children's rights in relation to the digital environment
[23] Recommendation of the Council on Children in the Digital Environment

- provide effective remedies for harms suffered by children via the digital environment, introducing new measures if existing legal frameworks fail to protect children or provide effective remedies;
- promote responsible business conduct;
- define conditions under which Digital Service Providers may be held liable for illegal activity by, or illegal information from, third parties using their digital products and services, which harm children

The recommendation also calls for international collaboration, including the sharing of information about domestic policy approaches to children in the digital environment, developing shared frameworks that enable internationally comparable standards and agreement on the definition of risks and benefits.

5Rights recommends:

W) The government should adhere to the OECD's recommendation to introduce legal measures that "provide for age-appropriate child safety by design", by ensuring safety by design is set out on the face of the Bill and its principles underpin the duties, to effectively prevent, mitigate and effectively manage all risks, not only content risks.

X) The government should build on its international reputation in the vanguard of online safety by ensuring the Bill establishes a gold standard for regulatory approaches to child online safety.

EU Artificial Intelligence Act

The European Commission's Artificial Intelligence (AI) Act[24], published in April 2021, aims to ensure that artificial intelligence technologies are held to high standards of protection for health, safety and fundamental rights. It makes for ground-breaking legislation which both recognises and defends children's rights in the digital world.

The AI Act prohibits any "AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm". It sets out the standards of risk management for 'high risk' AI systems and requires that "specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children." This wording acknowledges that few technologies are actually intended for use by children, but nonetheless impact children in ways they may not know.

[24] EU Proposals for Artificial Intelligence Act

It highlights that "children have specific rights as enshrined in Article 24 of the EU Charter and in the United Nations Convention on the Rights of the Child (further elaborated in the UNCRC General Comment 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being."

5Rights recommends:

Y) The government must consider that technologies which may not engage directly with children can still have an impact on their rights and wellbeing.

Z) AI systems – including algorithms – must be firmly within the scope of the Bill, and referenced in the duties relating to children. Ofcom must have sufficient oversight powers to regulate and audit the AI systems of regulated services.

For more information please contact:
Izzy Wick | Director of UK Policy | izzy@5rightsfoundation.com

Building the digital world that young people deserve

Annex A

Any services that pose significant risks to children must be in scope of the Online Safety Bill. We propose the following amendment to the meaning of "regulated service" (clause 3) to ensure commercial pornography providers as well as app stores, e-commerce sites and commercial EdTech providers are subject to the online safety legislation.

Clause 3: Meaning of "regulated service"

(2) "Regulated service" means—
(a) a regulated user-to-user service, or
(b) a regulated search service.

5Rights recommends the addition of:

(c) all services likely to be accessed by children