

Home Office preparedness for Covid-19 (online harms)

5Rights Foundation

May 2020

Introduction

During the covid-19 pandemic, more children are online for more of the time,¹ and those children are more dependent on digital technology to conduct a wider variety of their activities and affairs. As a result of this increased use and dependency, those who wish to harm children online have more opportunities to do so, and the risks created by the design of digital services themselves are also magnified.²

It is important to note, however, that this crisis has not changed the *nature* of the risk that children and young people face online. Rather, as a letter from the Children's Charities' Coalition on Internet Safety (CHIS) put it this week, 'lockdown has amplified and under-scored longstanding shortcomings in the online environment.'³ When things go back to normal, whatever that normal looks like, the risks will not have disappeared. More children will still be online for more of the time. The people who wish to harm them will still exist, and likely in greater numbers. Digital services will still be designed in ways that intensify risk for children and young people, rather than mitigate it.

If the online protections the Government has promised had been in place before this crisis – including the Age Appropriate Design Code, the age verification of online pornography, and a statutory duty of care for online platforms – the reports and figures we detail below may not have looked quite so grim.

The most natural response to all this is for the Government to expedite and strengthen its proposals for the protection of children and young people online. This is also what is expected of them by the public, and parents in particular. Last week, Doteveryone revealed that only 19% of people think tech companies design their services with their best interests in mind,⁴ and 5Rights' own polling found that 90% of parents think it is important that internet companies are required to follow rules to protect children online.

Despite this, the Government has chosen to delay further its proposals to protect children online,⁵ and likely water them down.⁶ We congratulate the Home Affairs Select Committee on holding the Government to account for this and welcome the opportunity to submit evidence on behalf of children and young people.

¹ A Parents Together survey found that 48% of respondents children are spending more than six hours online each day, a near 500% increase since before the crisis: [Screen time rockets during covid-10 crisis](#), Parents Together, May 2020

² See: [Children at increased risk of harm online during covid-19 pandemic](#), UNICEF, April 2020

³ [CHIS letter](#), May 2020

⁴ [People, Power, and Technology](#), Doteveryone, May 2020

⁵ [New duty of care laws to protection children from online harm could be delayed to 2023](#), Telegraph, April 2020

⁶ [Online harms bill: Government accused of watering down safer social media plans](#), i, February 2020

The nature, prevalence and scale of online harms during the Covid-19 period

There has been a significant uptick in a range of online harms relevant to children and young people during pandemic. Anecdotally, 5Rights has received a far higher volume of inquiries from parent and teachers concerned about the risks that their children are facing online. This includes the following:

Increase in online child sexual exploitation and abuse

- In April 2020, the first full month in lockdown, the US National Center for Missing & Exploited Children (NCMEC) received 4.2 million reports of suspected child sexual exploitation, an increase of nearly 3 million from the same month in 2019.⁷ In the previous month, March 2020, reports were up 106% from March 2019.⁸
- The UK's Internet Watch Foundation (IWF) reported in May 2020 that there were more than 8.8million attempts to access child sexual abuse material from websites on its 'URL list' in just a single month.⁹
- InHope, a network of 47 national 'cybertiplines', state that reports of child sexual exploitation are up 30% globally during the pandemic.¹⁰
- Cybersecurity analysts Web-IQ reported a 200% increase in posts on known child sexual abuse forums that linked to downloadable images and videos on the surface web. In February, the firm identified 2,790 links that were 'highly likely to point to child abuse material'. This rose to 9,255 in March.¹¹
- Against this backdrop, reduced staff numbers mean that tech companies and law enforcement bodies are struggling to keep up. The Internet Watch Foundation (IWF) reported that the amount of child sexual abuse material removed from the internet having been flagged fell by 89% over a four-week period during lockdown.¹²

Cyberbullying

- Australia's eSafety Commissioner reported a 50% increase in incidents of cyberbullying during the first three weeks of lockdown.¹³
- Analysis of digital toxicity by AI start-up L1ght reported a 70% increase in hateful and abusive language among children and teens in March 2020.¹⁴

In-game spending/gambling

- There has been a reported "surge in spending" on online games during lockdown. Industry tracking firm NPD reported that spending on gaming jumped 35% in the US in March, expected to increase even more significantly in April.¹⁵

⁷ [Online child abuse complaints surpass 4 million in April](#), Forbes, May 2019

⁸ [Child Exploitation Complaints Rise 106% To Hit 2 Million In Just One Month: Is COVID-19 To Blame?](#), Forbes, April 2020

⁹ [Millions of attempts to access child sexual abuse online during lockdown](#), IWF, May 2020

¹⁰ [Child sexual abuse images and online exploitation surge during the pandemic](#), NBC News, April 2020

¹¹ [Online child abuse flourishes as investigators struggle with workload during pandemic](#), Telegraph, April 2020

¹² [Lockdown hampering removal of child sexual abuse material online](#), The Guardian, April 2020

¹³ [Experts around the world warn parents to be vigilant as cyberbullying increases during lockdown](#), Cybersmile Foundation April 2020

¹⁴ [Rising levels of online hate speech and toxicity during this time of crisis](#), L1ght, April 2020

¹⁵ [Nintendo's Animal Crossing leads lockdown boom in video gaming](#), Financial Times, April 2020

- Pokémon Go saw in-game spending jump 67% globally in a single week in March after it introduced updates to adjust the game to indoor play.¹⁶
- While gambling firms in the UK agreed to cease advertising on TV and radio, there has also been a reported uptick in the targeting of gambling ads online during lockdown.¹⁷ This is particularly concerning given the evidence on children's exposure to gambling ads online. In March 2020, Ipsos Mori and GambleAware published research finding that more than one in four 11-17-year-olds had seen gambling ads on social media or elsewhere online in the past two weeks.¹⁸

Misinformation

- In May 2020, Facebook CTO Mike Shroepfer confirmed that there has been 'a huge increase in misinformation that we consider dangerous' during the Covid-19 pandemic.¹⁹ In the same month, the US-based Centre for Infectious Disease Research and Policy announced that its 'Facebook studies reveal that science-mistrust is winning on vaccine messaging.'
- Children and young people tend to be under-associated with the impact of misinformation online, despite being disproportionately impacted by its spread. For instance, while children and young people appear to be less susceptible to the coronavirus, they have always been (and will continue to be) the primary victims of the anti-vax movement. The greater the spread of anti-vax misinformation now, the more children who will be at risk if and when a vaccine for coronavirus is made available.²⁰

Online pornography

- Pornhub announced a record 12% increase in worldwide traffic during March, and significantly higher in countries that were in lockdown during the period (57% in Italy, 39% in France, 61% in Spain).²¹
- This is the context of consistent evidence of children's exposure to pornography online,²² as well as evidence that young men are seeking out sexual images and videos of children after being desensitised by intense or prolonged exposure to pornography.²³
- Analysis by the India Child Protection Fund (ICPF) found that interest/demand for child sexual abuse material had nearly doubled early in the pandemic, citing data from Pornhub that showed significant increases in search terms such as 'child porn', 'sexy child', and 'teen sex videos'.²⁴

¹⁶ [Pokémon Go spending jumps 67% after indoor play adjustments](#), Mobile Marketer, March 2020

¹⁷ [Coronavirus: 'I'm being bombarded with gambling ads'](#), BBC News, May 2020

¹⁸ [Final synthesis: the effect of gambling marketing and advertising on children, young people, and vulnerable adults](#), Ipsos Mori and GambleAware, March 2020

¹⁹ [Facebook upgrades its AI to better tackle misinformation and hate speech](#), TechCrunch, May 2020

²⁰ [Facebook studies reveal that science-mistrust is winning on vaccine messaging](#), Centre for Infectious Disease Research and Policy, University of Michigan, May 2020

²¹ Urgent action needed as rise in porn site traffic raise abuse fears, The Guardian, March 2020

²² See e.g. [Pornography one click away from young children](#), BBC News, September 2019

²³ Rise of paedophilia among young men desensitised by Pornhub, Metro, April 2020

²⁴ [ICPF report warns of sharp increase in demand for child pornography during lockdown](#), Times of India, April 2020

Steps that could be taken to mitigate these concerns

While we welcome the Government's recent efforts to provide information to parents and children about staying safe online,²⁵ the concerns above are addressed more effectively 'upstream', in the design and development of digital services themselves. Safety information is not a replacement for a digital environment that is safe by design, nor are unrealistic demands on the vigilance of parents²⁶ a replacement for digital services that anticipate the risks they pose to children, and mitigate them by default.

In order to ensure that digital service providers take this responsibility seriously, the Government must introduce robust, enforceable legislation. We address the shape of this legislation as it relates to the Government's online harms proposals below, but we want to draw the Committee's attention to the Age Appropriate Design Code, which is in a position to provide online protection for children and young people much sooner.

Age Appropriate Design Code

The Age Appropriate Design Code is a world-leading piece of regulation that gives children and young people the privacy protection they need to stay safe online. Data drive many norms of the digital world, and the way children's data are collected, shared, and used impacts significantly not just on their digital experience, but also on their wider lives. As such, the Code offers a significant and welcome change in how children and young people are protected and supported in the digital age. It guarantees them a high-level of privacy by default, makes services more responsible for content recommendations made on the basis of children's data, and strengthens requirements around age assurance/verification.

The Information Commissioner was required to prepare the Code by s123 of the Data Protection Act 2018. Under s.125, the Secretary of State is required to lay the Code in Parliament "as soon as reasonably practicable". Now that the Code has returned from its three-month EU 'standstill' period with no comments or objections, there are no reasons to delay.

In order for the Code to take effect before the summer, it will need to be laid in both Houses by 10 June. Following an additional 21-day period, it will enter a year-long transitional period to help services comply. At the earliest, therefore, children and their parents will still have to wait over a year to enjoy the protections that the Code provides. If the Government delays the laying of the Code past 10 June, the Code cannot complete its time in Parliament until the Autumn, wasting another two or three precious months.

In evidence to the House of Lords Democracy and Digital Technologies Committee in May 2020, Digital Minister Caroline Dinenage MP said that the Department was in negotiations with the parliamentary authorities about when the Code could be laid. Given, however, that the Code is subject to the negative procedure for statutory instruments, and as such does not require any significant parliamentary or departmental time, we do not see why the Code cannot be laid immediately. Indeed, many companies have already started work in anticipation of the Code.

²⁵ [Coronavirus \(Covid-19\): staying safe online](#), UK Government, April 2020

²⁶ Not least those parents who are juggling supervision of their children with home-schooling and full-time job

The adequacy of the Government’s Online Harms proposals to address issues arising from the pandemic, as well as issues previously identified.

We remain concerned about indications that the Government is preparing to water down its proposals for the protection of children and young people online. As we outline above, this is both counter-intuitive and dangerous given the increased risk that children and young people face during and because of the pandemic. We summarise below our view on what online harms legislation needs to require of companies and the extent to which we believe the Government’s proposals cover them. This is based on the Online Harms White Paper, the initial consultation response published in February, and comments made by Ministers in various parliamentary committees over the last few weeks.

Minimise risk by design and default

Properly fulfilled, a duty of care means anticipating and mitigating risk, in advance and on an ongoing basis, during the design and development of a product or service.²⁷ It is important, of course, that providers have systems in place to respond to harmful incidents if and after they occur, but the gold-standard is to build products and services that minimise the risk of those incidents happening in the first place, by design and default.

In practice, this means that online harms legislation should focus on holding platforms to account for their recommendation algorithms,²⁸ user journeys, age-assurance mechanisms, and default settings, not just their reporting tools and take-down procedures. In its initial response to the Online Harms White Paper, the Government stated that:

“the duty of care [will] be designed to ensure that all companies have appropriate systems and processes in place to react to concerns over harmful content and improve the safety of their users – from effective complaint mechanisms to transparent decision-making over actions taken in response to reports of harm.”

While such ‘downstream’ systems and processes are necessary, they are not a replacement for systems and processes that address risk ‘upstream’.

Address content, contact, conduct, and contract risks

In that initial consultation response, ‘content’ is mentioned no fewer than 99 times. Comparatively, ‘contact’, ‘conduct’, and ‘contract’ risks receive little to no attention.²⁹

Children’s exposure to harmful and adult content is a key concern, but children are also exposed to unsolicited, unsupervised contact with other users who may wish to harm them; they are encouraged to share their personal information more widely and in more detail than they otherwise would or could; and they are subject to commercial pressures and contractual relationships that are not appropriate for their age. In each case, these risks are

²⁷ Note: the prevention of foreseeable harm is the essence of a duty of care. See: [Online harm reduction – a statutory duty of care and regulator](#), Woods/Perrin, 2019

²⁸ See: [Regulating Recommending: Motivations, Consideration, and Principles](#), Cobbe/Singh 2019; [Online content: to regulate or not to regulate, is that the question?](#), Vermeulen, 2019

²⁹ [Online Harms White Paper – initial consultation response](#), UK Government, February 2020

intensified or mitigated by the way a service or feature is designed. Online harms legislation must require the anticipation and mitigation of all these types of risk, not just ‘content’ risks.

Child impact assessments

The Government has repeatedly emphasised the importance of protecting children and young people in particular as part of its online harms proposals. We welcome that emphasis, but ask that under new online harms legislation, providers of online platforms be given a specific duty to assess the impact of their services on children and young people, in advance and as distinct from other users. Providers should be ready to account for those assessments and for the steps they have taken to eliminate or mitigate the risks to children and young people they have identified.

Given the speed at which technology evolves and the continuous deployment of software updates and changes, such assessments of impact should be ongoing. This is in line with Article 17 of the UN’s Guiding Principles for Business and Human Rights, which states that due diligence *‘should be ongoing, recognising that the human rights risks may change over time as the business enterprise’s operations and operating context evolve.’*³⁰

The Government should also clarify that children and young people includes everyone under the age of 18. To date, child specific online protections have tended to apply only to children under the age of 13, and even these come in the form of flimsy age-gates that mistakenly seek to protect children from the digital environment, rather than protect them within it. Protection for children of different ages need not be the same, but all minors should be entitled to appropriate protection on account of the vulnerabilities associated with their age.

Uphold community standards and other published terms

The Government has committed to ‘holding companies accountable for enforcement of their own standards’, both in the White Paper and in its initial consultation response. This is an important aspect of the duty of care and one that 5Rights first suggested in our January 2019 report *Towards an Internet Safety Strategy*.³¹ Our recommendation was made on the back of the workshops we hold with children and young people, who consistently tell us that community standards are inconsistently upheld, there are no meaningful consequences or punishments for violations, and reporting concerns often result in no acknowledgement or action.

Crucially, community standards and other published terms, including age restrictions, enable children or their parents to decide if a service is appropriate and to anticipate the risks it might pose. They are therefore fundamental to the safety of children online and to their ability to navigate the digital environment confidently and independently.

Asking companies to ‘say what they do and do what they say’ is only a baseline, however. Companies cannot be left to set all their own standards themselves, and the role of

³⁰ [UN Guiding Principles on Business and Human Rights](#), UN, 2011

³¹ [Towards an Internet Safety Strategy](#), 5Rights, 2019

regulation is to ensure that companies do what they otherwise might not, in the public interest. So, regulations to hold companies to account for how they uphold their own standards is welcome and important, but it must come as part of a broader package.

About 5Rights Foundation

The digital world was never imagined as an environment in which childhood would take place. It was invented by adults, for adults and designed with the idea that all users are equal. But if all users are treated equally, then children and young people are treated as adult.

5Rights Foundation exists to make systemic changes to the digital world to ensure it caters for children and young people, by design and default. We advocate for enforceable regulation and international agreements that allow children and young people to thrive online. We develop technical standards and protocols to help businesses redesign their digital services with children and young people in mind. We publish and lead across our four priority areas: Design of Service, Child Online Protection, Children and Young People's Rights, and Data Literacy.

For further evidence or information, please contact 5Rights Policy Lead Jay Harman on jay@5rightsfoundation.com or 07970 393 680.