Government response to the Internet Report by the Independent Inquiry into Child Sexual Abuse

November 2020

Introduction

1. Protecting children online is at the heart of the Government's online harms agenda, and wider Government priorities. We want to deliver the most comprehensive and coherent approach to keeping children safe online.

2. The Government's proposed approach to improving internet safety generally was set out in the Online Harms White Paper[1], published in April 2019. The White Paper put forward ambitious plans for a new system of accountability and oversight for tech companies, moving far beyond self-regulation. It was proposed that a new regulatory framework for online safety would make clear companies' responsibilities to keep UK users, particularly children, safer online with the most robust action to counter illegal content and activity. This would be overseen by an independent regulator which would set clear safety standards, backed up by reporting requirements and effective enforcement powers.

3. The proposals in the White Paper were the subject of a public consultation which ran from April to July 2019. In February 2020 the Government published its initial response to the consultation[2], providing an overview of the responses received and an indication of the direction of travel in a number of key areas raised as overarching concern across some responses. In particular, the response stated that the Government was minded to appoint Ofcom as the new regulator.

4. The Queen's Speech on 19 December 2019, which set out the Government's legislative priorities for this parliamentary session, included a commitment to develop legislation to improve internet safety for all in order to make the UK the safest place in the world to go online.

5. Government will publish later this year the full response to the White Paper which will include further details on the proposals to online harms regulation.

---

[1]

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

[2] https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

Response to the recommendations

6. The Government is very grateful to the Inquiry for its Internet Investigation Report and the insight it provides. The Home Office and Department for Digital, Culture, Media and Sport (DCMS) have worked closely together to consider carefully the Inquiry's recommendations. The Government's response to each is set out below.

Recommendation: Draft child sexual abuse and exploitation code of practice

The Government should publish, without further delay, the interim code of practice in respect of child sexual abuse and exploitation as proposed by the Online Harms White paper (published April 2019).

---

7. The Online Harms White Paper committed the Government to working with law enforcement agencies and other relevant bodies to produce interim codes of practice on terrorism and child sexual exploitation and abuse (CSEA) due to the serious nature of these harms. The interim codes are voluntary and intended to bridge the gap until the regulator is operational and ready to produce its own codes.

8. The interim code of practice on CSEA will be published alongside the full Government response to the White Paper referred to in paragraph 5 above.

Recommendation: Pre-screening of images before uploading

The Government should require industry to pre-screen material before it is uploaded to the internet to prevent access to known indecent images of children.

---

9. In March 2020, the UK, US, Australia, Canada and New Zealand launched the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse. The principles were developed in consultation with six leading technology companies and a wide variety of experts from industry, civil society and academia, as well as the WeProtect Global Alliance (WPGA) [see paragraphs 17-23 below]. The principles aim to provide a framework to combat online CSEA, and are intended to drive collective action.

10. The aforementioned interim code of practice on tackling CSEA builds upon the Voluntary Principles which set out the UK Government's expectation that all companies will prevent access to known child sexual abuse material. The first principle is that companies seek to prevent known child sexual abuse material from being made available to users or accessible on their platforms and services, take appropriate action under their terms of service, and report it to appropriate authorities. Pre-screening is one means of preventing access, recognising that this threat and the response that it requires may vary depending on the type and nature of the service offered.

Recommendation: Age verification

The Government should introduce legislation requiring providers of online services and social media platforms to implement more stringent age verification techniques on all relevant devices.

11. The Government's initial response to the White Paper, published in February 2020, outlines our proposals for tackling online harms and delivering a higher level of protection for children than for the typical adult user. We set out the expectation that companies would use a proportionate range of tools, including age assurance and age verification technologies, to prevent children from accessing age-inappropriate content such as online pornography, and to protect them from other harms.

12. The Government has been clear that we expect companies to use a range of tools now to protect children online and that we expect that age assurance methods, including age verification, will play a key role in the online harms regulatory framework. We are committed to the UK becoming a world leader in the development of online safety technology and to ensuring that companies of all sizes have access to, and adopt, innovative solutions to improve the safety of their users. We are working closely with stakeholders to consider what could be delivered ahead of, and through, the online harms regulatory framework.

13. Over the last 12 months DCMS has supported the 'Verification of Children Online' (VoCO) child safety research project. The report on the project's second phase was published this month. This joint GCHQ, DCMS and Home Office project responds to the technical challenges associated with providing children with a greater level of protection from online harms and explores the feasibility of identifying child users online. The VoCO project has attempted to capture the experiences and needs of children, parents and platforms to identify what support and incentives are needed for platforms to start age assuring their users.

14. Knowing which users are children, and what age band they are in, is critical to protecting children online. If online services know which of their users are children, they are able to provide them with a higher level of protection, including preventing access to age inappropriate content. Age assurance is the term given to the broad range of technical measures that can be used by an online service to establish the age of their users. The VoCO project showed that there are a range of age assurance methods, supported by different data sources, that companies can use to assess the age of their users. Different age assurance methods provide differing levels of confidence in the age of the child. Age verification is one type of age assurance measure and provides the highest level of confidence in the assessed age of the child. Current age verification measures are effectively a full identity check.

15. The VoCO report sets out that the age assurance method used by a platform should be proportionate to the likely risk posed to a child by that platform. The report suggests that in assessing risk, companies should take into account factors such as the type of content hosted on the service, its features, and its user base. This approach is aligned with the risk-based and proportionate approach to tackling online harms that is set out in the Online Harms White Paper, published in April 2019.

16. In addition, ahead of the implementation of the new regulatory framework, the Government will continue to encourage companies to take early action to address online harms. The White Paper sets out high-level expectations of companies, including specific expectations in relation to certain harms, such as protecting children from accessing inappropriate content online. Ahead of legislation, the Government will publish guidance on embedding 'safety by design' principles into the design and development of online products and services. This will serve as best practice for reducing online harms for users, especially children. We are also developing a 'one-stop shop' to give companies practical guidance on keeping children safe online. This will help companies understand their existing legal responsibilities and learn from best practice.

Recommendation: Removal of images

The Government should press the WeProtect Global Alliance to take more action internationally to ensure that those countries hosting indecent images of children implement legislation and procedures to prevent access to such imagery.

---

17. The WPGA is a global movement, founded by the UK Government, bringing together the influence, expertise and resources required to transform how online child sexual exploitation is dealt with worldwide. As of October 2020, membership stands at 98 countries, 39 companies, and 41 civil society organisations.

18. The UK Government was the sole funder of the WPGA from its inception in 2016 until 31 March 2020, at which point the initiative relaunched to become an independent body. The WPGA's achievements while funded and supported by the UK Government include:

- Four international summits, bringing together leading figures from across governments, civil society and industry to raise awareness of the threat and required response to online child sexual exploitation, most recently in December 2019 in partnership with the African Union;
- A Model National Response (MNR) document (2015)[3]. The MNR is divided into 21 capabilities, and acts as a blueprint for establishing and delivering a coordinated national response to tackle online child sexual exploitation. Of particular relevance to this recommendation are capabilities 3 and 12. Capability 3 sets out examples of good legislative frameworks and capability 12 explores the need for a dedicated hotline to enable the reporting of illegal material, including child sexual abuse material, hosted online;

---

[3] https://www.weprotect.org/the-model-national-response

- Two Global Threat Assessments (2018[4]; 2019[5]) which draw together international expertise to develop the collective understanding of the threat of online child sexual exploitation;
- A Global Strategic Response framework[6] to guide and coordinate action on tackling this crime at a global and regional level;
- An event in November 2018, co-sponsored by the WPGA and the Child Dignity Alliance and hosted by Microsoft, to discuss new efforts led by the technology industry and others in combatting child sexual exploitation online, alongside Microsoft's '360 Cross-Industry Hackathon' focused on tackling the same issue; and
- The promotion of the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, referenced in paragraph 9.

19. Supported by a range of philanthropic donors, the WPGA will continue to lead in the fight against online CSEA. The UK Government is a permanent member of its new management board, and as such continues to have a degree of strategic leadership that allows us to help direct the WPGA's prioritisation of its work, including online child sexual abuse and engagement with partner countries and technology companies in particular.

20. The UK Government will continue to work collaboratively with the WPGA to continue to make combatting indecent images of children, grooming and live streaming a top priority, both through its board meetings and by ensuring the WPGA further develops and disseminates key resources, such as the aforementioned MNR, Global Threat Assessment and Global Strategic Response framework.

21. The WPGA is working toward a Global Summit in 2021, to be held in Brazil, to keep this issue on the agenda for high-level representatives globally. By engaging with regional organisations such as the African Union at the December Summit, as well as with Latin America, the Association of South East Asian Nations, the European Union and others - and with individual countries - the WPGA is in a unique position to ensure that the MNR in particular becomes the fundamental piece of guidance used to develop workable and effective legislation to help in that fight.

22. Although the launch of the independent WPGA was made more difficult by the COVID-19 lockdown and response shortly after, plans for an ambitious set of objectives and deliverables are still in place. As a point of liaison between governments, law enforcement, civil society and the technology industry, the WPGA is also uniquely placed to drive commitment and endorsement of the Voluntary Principles. The WPGA will connect subject matter experts to share best practice and analyse the evolving threat environment to identify gaps in the global response.

4

https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5e4ed6110f2fa76663e58a83/1582224937659/Global+Threat+Assessment+2018+-+English

5

https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef23016423cf/1575930642519/FINAL+-+Global+Threat+Assessment.pdf

6

https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deeccd9ab886c6b1e41cf9b/1575931097730/FINAL+-+Global+Strategic+Response+.pdf

Conclusion

23. The Government will keep the Inquiry updated on progress in this area and the implementation of this programme of work.