Department for Culture, Media & Sport

Lord Parkinson of Whitley Bay
Minister for Arts & Heritage
1st Floor
100 Parliament Street
London SW1A 2BQ

E: enquiries@dcms.gov.uk

www.gov.uk/dcms

29 June 2023

To: All Peers

INT2023/07234/DC

My Lords,

ONLINE SAFETY BILL: FOLLOW UP TO DEBATE ON DAYS 8–10 OF COMMITTEE

Many thanks to those who took part in the eighth, ninth, and tenth days of Committee on the Online Safety Bill. I am pleased to provide further information below on a number of issues raised.

I would also like to take the opportunity to explain how the duty in the Bill requiring in-scope services to conduct a children's access assessment will align with the Age Appropriate Design Code, following the debate we held on the second day of Committee. I have set this out in detail in **Annex A**.

DAY EIGHT

Lord Bethell asked for clarification about where the outcomes of the child safety duties are set out in the Bill.

The Bill sets clear outcomes for providers to protect children from harmful content and activity on their services. The key outcomes that providers in scope of Part 3 and Part 5 must achieve include the following:

- ***In Part 3 – for user-to-user services:***
  - providers must **prevent children from accessing primary priority content** and **protect children in age groups judged to be at risk of harm from other content that is harmful to children** (clause 11(3)(a)) and 11(3)(b));
  - they must also **effectively manage and mitigate the risks of harm to children in different age groups**, as identified in the most recent children's risk assessment and **mitigate the impact of harm to children in different age groups presented by content which is harmful to children present on the service** (clause 11(2)(a)) and 11(2)(b)).

- ***In Part 3 – for search services:***
    - providers must **minimise the risk of children of any age encountering search content that is primary priority content** which is harmful to children and **minimise the risk of children in age groups judged to be at risk of harm from other content that is harmful to children** from encountering search content of that kind (clause (25(3)(a)) and 25(3)(b));
    - they must also **effectively manage and mitigate the risks of harm to children in different age groups**, as identified in the most recent children's risk assessment and **mitigate the impact of harm to children in different age groups presented by search content that is harmful to children** (clause 25(2)(a)) and 25(2)(b).
- ***In Part 5:***
    - there is a duty to ensure that children are 'not normally able to encounter' regulated provider pornographic content (clause 72(2)), a similar test as would have applied under Part 3 of the Digital Economy Act 2017.

Since the debate on this issue, we have had discussions about the changes the Government is making to strengthen the Bill's duties in relation to children's access to pornography and other categories of primary priority content that is harmful to children. I have written separately setting out the Government's proposed changes to the Bill, including in relation to this issue. The proposed changes will ensure that children are prevented from accessing pornography, wherever it is available, using measures that are highly effective in a consistent manner across all services. We hope you can support these amendments at Report stage.

Lord Bethell asked for reflections on how the use of copyright and contract law could be improved when dealing with protecting the rights of those who find their images wrongly used on pornographic sites, particularly children.

The Bill has been designed to tackle the growing and evolving threat of child sexual exploitation and abuse online. The distribution of indecent images of children is a separate issue to the rights of performers in copyright and contract law, and in no way should these images be considered as pornography. The Government classifies such activity as a child sexual exploitation and abuse offence, and the law is very clear on this issue. Under the Protection of Children Act 1978 (as amended), the UK has imposed an absolute prohibition on the taking, making, circulation, and possession with a view to distribution of any indecent photograph (or pseudo-photograph) of a child under 18 and these offences carry a maximum sentence of 10 years' imprisonment. Section 160 of the Criminal Justice Act 1988 also makes the simple possession of indecent photographs (or pseudo-photographs) of children an offence and carries a maximum sentence of 5 years' imprisonment. In addition, section 62 of the Coroners and Justice Act 2009 created a criminal offence to make illegal the possession of non-photographic visual depictions of child sexual abuse, including 'Hentai' cartoons and computer-generated images of child abuse, with a three-year maximum prison sentence.

Under Part 3 of the Bill, child sexual exploitation and abuse offences (including those considered above) have been listed as priority offences, meaning that content and activity amounting to these offences are subject to the most stringent duties. All services in scope of Part 3 must take proactive, preventative measures to tackle this criminal content and behaviour on their services. Ofcom will set out in codes of practice the steps that companies can take to comply with their illegal safety duties, including by a dedicated code of practice on tackling child sexual exploitation and abuse. Reflecting the seriousness of this harm, the Bill also includes a power enabling Ofcom to require companies to use accredited technology to detect child sexual exploitation and abuse material, including on private communications. Providers must also report child sexual exploitation and abuse content they detect on their platforms to

the National Crime Agency, if this has not already been reported to an appropriate agency. Providers in scope of Part 5 are publishers which directly control the material on their services, and can therefore already be held liable for child sexual exploitation and abuse offences captured by the criminal law.

In addition, the Government is committed to tackling the non-consensual sharing of intimate images, which is also a separate issue to the rights of performers in copyright and contract law. Under section 33 of the Criminal Justice and Courts Act 2015, it is already an offence to share private sexual photographs and films without the consent of the individual appearing in the photograph or film and with intent to cause them distress. The Government will also introduce new offences in the Bill relating to sharing and sending intimate images without consent. These new offences include the sending and sharing of 'deepfake' pornography, as well a new 'base offence' which criminalises someone for sharing an intimate image without consent. These offences will be priority offences for all Part 3 services in the Bill, which will include some of the most popular commercial pornography services. As I mentioned during the debate, these new offences will also apply to providers in scope of Part 5, and they will be criminally liable for any non-consensual intimate images published on their services.

As I have outlined, the Bill has been designed to introduce robust requirements on providers to tackle child sexual exploitation and abuse and the non-consensual sharing of intimate images. This is a separate matter to copyright and contract law, which gives performers based in the UK the right to authorise the making of a recording of their performances. Consent before publication is usually dealt with through contractual agreements between the performer and the creator. If the performer sought to remove this consent, then the outcome would depend on the contractual arrangements he or she signed at the time. Any works recorded and made available to the public without the performer's consent would constitute an infringement of the performer's rights. As a private right, it is for the performer to enforce this, not this regulatory regime.

DAY NINE

Lord Knight of Weymouth asked whether Ofcom's annual transparency reports will be laid before Parliament and debated.

Under clause 147, Ofcom is required to produce its own annual transparency report, which must include a summary of conclusions drawn from providers' transparency reports, along with Ofcom's view on industry best practice and other appropriate information. While there is no legislative requirement for Ofcom's transparency reports to be laid before Parliament, they will be published, so will be subject to public scrutiny.

Under paragraph 12 of the Schedule to the Office of Communications Act 2002, however, Ofcom is already required to produce an annual report on the carrying out of its functions and to send it to the Secretary of State. This annual report will report on Ofcom's carrying out of its functions, including its online safety functions such as transparency reports. The Secretary of State for Science, Innovation and Technology is required to present Ofcom's annual report and accounts before both Houses of Parliament as well as to the devolved assemblies.

Further to this, clause 161 of the Bill requires the Secretary of State to undertake a comprehensive review of the effectiveness of the Online Safety regulatory framework, and the report on the outcome of this review must also be laid before Parliament. The review must assess the effectiveness of the regulatory framework in ensuring that the systems and processes used by services provide transparency and accountability to users.

I hope this provides reassurance that Ofcom is accountable to Parliament in how it exercises its functions and that, through Ofcom's existing reporting requirements and the Secretary of State's review, Parliament will be able to give due consideration to the framework's approach to transparency.

Lord Stevenson asked for clarification about what is covered in relation to the 'scope' of terms of service in the transparency reporting requirements.

It is important that Ofcom can request information about the scope of terms of service, as well as about their application. Following careful consideration of the points raised by Lord Stevenson during Committee stage, we are pleased to be making changes which will expand the transparency reporting powers to allow Ofcom to require information relating to the "scope" of user-to-user providers' terms of service, and search service's public statements of policies and procedures. We are also enabling ofcom to require information about the "formulation" and "development" of terms of service, which will allow for valuable insights such as the factors companies have taken into account in developing their terms of service. I have written separately detailing these changes alongside other amendments made ahead of Report stage.

Lord Stevenson requested clarification on whether Section 110 Notices apply to terrorism content and referred to safeguards under the Regulation of Investigatory Powers legislation.

Under clause 111, Ofcom is only able to require the use of accredited technology on private communications for the sole purpose of identifying, taking down, and preventing users from encountering child sexual exploitation and abuse content. The only other type of content in relation to which Ofcom can use this power is terrorism content – but it can only require the use of technology to tackle terrorism content on *public* communications. (Lord Stevenson's amendment 210A only sought to introduce special provisions for journalistic material in relation to *private* communications, so this would not relate to notices to deal with terrorism content.)

The powers in the Investigatory Powers Act 2016 serve different purposes to those within the Online Safety Bill. The different legal safeguards in the Investigatory Powers Act reflect the potential intrusion by the state into an individual's private communications.

The Investigatory Powers Act provides additional safeguards for confidential journalistic material and for sources of journalistic information. These apply where there is a belief that journalistic material may be part of the communications in question, or when identifying or confirming a journalistic source is the purpose, or one of the purposes, of the warrant/authorisation. Clause 111 of the Online Safety Bill does not give Ofcom the power to require that it be given access to content, including potentially journalistic content, on private channels. Instead, the Bill empowers Ofcom to ensure that online services are taking the appropriate steps to keep their own users safe from the most serious harm.

Strong safeguards regulate the use of this power. To ensure that only child sexual exploitation and abuse content is detected on private communications, any technology required under clause 111 must be accredited by Ofcom as being highly accurate. Minimum standards of accuracy will reduce the risk of both false positives and false negatives, including the risk that content is incorrectly flagged for moderation or removal, thus helping to protect all users' rights to privacy and freedom of expression.

DAY TEN

Baroness Newlove asked how we can ensure that coroners keep up with training on social media

The Chief Coroner for England & Wales has statutory responsibility for maintaining appropriate arrangements for the training of Coroners. This is independent of Government, and exercised through the Judicial College; the training is mandatory. The Chief Coroner will consider issuing non-statutory guidance and training for coroners about social media as appropriate, subject to the prioritisation of resources. We are confident that this well-established framework provides an effective means to provide coroners with training on online safety issues.

Baroness Kidron asked about business disruption measures against out-of-scope services

Ofcom can apply to the courts for business disruption measures in relation to regulated services. The Government is confident that the Bill will capture the vast majority of harmful online content, and that this approach targets Ofcom's enforcement powers in an effective and proportionate way.

While these measures cannot be applied to out-of-scope services, such services may be required to take steps if they operate as an access facility or an ancillary facility for a non-compliant regulated service. In such cases, Ofcom will be able to apply to the courts for that third-party service to take steps to withdraw, adapt, or manipulate its service in such a way as to disrupt, or impede access to, the regulated service in question.

Law enforcement agencies are already able to take steps to tackle the producers or publishers of illegal content.

Lord Allan of Hallam asked what work has been undertaken in the UK to ensure researchers can safely receive and use data for research purposes

As set out in the debate, the Bill will require Ofcom to undertake a report on researchers' access to information. In recognition of the importance of this issue, we are pleased to be making amendments to require Ofcom to publish its report into researchers' access to information within 18 months, rather than two years. Furthermore, Ofcom will now be required to publish guidance on this issue, including guidance on how to improve access for researchers in a safe and secure way.

Ofcom's report will include an assessment of the legal issues which currently constrain the sharing of information for research purposes, such as the regulation of personal data, and how greater access to information might be achieved. As part of its investigation, Ofcom will be required to consult the Information Commissioner's Office (ICO), and will take into account any guidance the ICO has issued.

Indeed, the ICO has issued guidance about the research provisions in the UK General Data Protection Regulation and the Data Protection Act 2018, which allow organisations to process personal data for research purposes. The guidance is aimed at those with specific data protection responsibilities in organisations undertaking research, archiving or processing for statistical purposes. This guidance covers research-related data-processing, the principles and grounds for data-processing, and the appropriate safeguards which need to be in place before processing personal data for research purposes.

Further to this, the Data Protection and Digital Information Bill will provide greater clarity to researchers on compliance with data protection legislation. By making the law simpler to understand for both researchers and data subjects, that Bill will both foster trust and transparency and facilitate life-enhancing research.

Lord Allan questioned whether VPNs are in scope of access restriction orders

Any person who provides an access facility (as set out in the definition of 'access facility at clause 135 (10)) which it is able to withdraw, adapt, or manipulate in such a way as to impede access to a regulated service can be subject to an access restriction order. This definition would cover virtual private networks (VPNs), in cases where such networks would be able to impede access to specific sites. In practice, this means that VPNs could be ordered to restrict access to non-compliant services. This broad definition ensures that all relevant services are captured and provides Ofcom with the flexibility to identify on a case-by-case basis where business disruption measures will be best targeted to achieve their aim.

Lord Moylan asked about the interaction of Clause 162 with the illegal content duty

Lord Moylan raised concerns about the interaction of the false communication offence (clause 162) with the Bill, and suggested that the new offence could lead to platforms excessively removing content in seeking to comply with their illegal content duties. The Government believes that clause 162 is a necessary update to the existing communications offences. The new offence will capture knowingly false communications, with an intention to cause non-trivial physical or psychological harm. Importantly, the sender must have no reasonable excuse for sending the communication for an offence to have been committed.

When supervising providers' compliance with their duties, Ofcom will not penalise providers for individual content moderation decisions. Rather, the aggregate performance of systems and processes, the way they are designed, and the overall approach they take to assessing and dealing with content will be relevant. This is important, as this approach reduces the risk that the framework will create incentives for the unwarranted removal of borderline content.

The Bill also places duties on in-scope platforms to have particular regard to the importance of protecting freedom of expression when fulfilling their duties. For example, platforms could safeguard freedom of expression by ensuring human moderators are adequately trained to assess contextual and linguistic nuance to prevent the over-removal of content.

In terms of identifying illegal content, platforms will be required to remove content where they have reasonable grounds to infer that all the elements of an in-scope offence, including any necessary mental elements (e.g. intent) are present, and that no defence is available. Specific provision at clause 173 reduces ambiguity about how these elements should be treated, reducing the risk that companies either remove too much or too little content. Ofcom will provide guidance to providers about how companies should approach judgements about whether content is illegal content.

Lord Allan asked what the Government thinks should happen to non-regulated services outside the UK's jurisdiction that promote self-harm content which breaks the law

It is worth noting that the offence of encouraging or assisting serious self-harm will apply to any communications which meet the threshold in the offence, regardless of whether they were shared on a site outside the scope of the Bill.

In terms of UK jurisdiction, Government policy generally on the jurisdiction of our courts is that criminal offending is best dealt with by the criminal justice system of the state where the offence occurred. The criminal law of England and Wales, and those of Scotland and Northern Ireland, do not ordinarily extend to conduct outside the United Kingdom. However, Government amendments 268CA and 268EA amended what is now clause 168 of the Bill to provide for the extraterritorial application of the new offence of encouraging or assisting serious self-harm, and to give courts in the UK jurisdiction to deal with the new offence if it is committed outside the UK by an individual habitually resident in the UK. This is the approach recommended by the Law Commission to ensure that criminal liability could not be avoided by those to whom the offences would ordinarily apply (because, for example, they are habitually resident in the UK), by sending communications while temporarily outside the jurisdiction.

User-to-user services in scope of the Bill will also have duties to protect children from encountering harmful content by means of their service, and not just on their service itself. This could include protecting children from being directed to harmful content or activity on other sites. Additionally, many people access self-harm content through search services. Under the Bill, search services will need to take steps to keep their users safe from illegal content or harmful content affecting children, in or via search results. Together, these duties will play a key role in reducing traffic to websites which encourage or assist serious self-harm.

Baroness Finlay of Llandaff asked whether there had been prosecutions under the Suicide Act

The threshold for prosecuting an offence of encouraging or assisting suicide under the Suicide Act 1961 is high but there have been some successful prosecutions. The 1961 Act applies to encouragement or assistance given online as well as offline.

Baroness Finlay asked whether a person who creates an algorithm that disseminates content that meets the threshold in the self-harm offence will be captured

The effect of sub-section (1) of the self-harm offence (clause 167) is that a person commits an offence if he or she does a relevant act capable of encouraging or assisting the serious self-harm of another person; and his or her act was intended to encourage or assist the serious self-harm of another person. Sub-section (7) makes clear that an offence under subsection (1) may be committed online where someone forwards another person's direct message or shares another person's post, as well as when he or she publishes a physical document such as a pamphlet or booklet. This means that an offence will be committed even where the person who does the relevant act did not actually create the material or content being communicated.

Algorithms are designed automatically to send people material which may be of interest to them. It seems unlikely that if a person merely creates an algorithm and does not himself or herself send, transmit or publish the communication (for example), he or she could be said to be undertaking a 'relevant act'. However, every case will turn on its specific facts, and if the circumstances are such that a person's action does constitute 'a relevant act capable of encouraging or assisting the serious self-harm of another person' and that act is intended to encourage or assist the serious self-harm of another person, then the creator of the algorithm will be captured.

It was suggested that sub-section (10) of the new offence negates the effect of sub-section (7). That is not the case. The purpose of sub-section (10) is to provide an exemption for internet service providers where they merely provide a means by which others can access the internet. Similar exemptions apply to the false and threatening communications offences (under clause 165(4)), to the offence of sending flashing images electronically (under clause 166(6)) and to the existing offence of encouraging or assisting suicide (under section 61 of and Schedule 12 to the Coroners and Justice Act 2009).

Many thanks to all the Noble Lords who raised points and questions over the ten days of debate in Committee. I look forward to continuing to work with you as our deliberations are reported back to the House.

With best wishes,

Lord Parkinson of Whitley Bay
Minister for Arts & Heritage

Annex A: The Online Safety Bill's alignment with the Age Appropriate Design Code

Concerns were raised on the second day of Committee about how the duty for in-scope services to conduct a children's access assessment in the Online Safety Bill aligns with the duty in the Data Protection Act 2018 regarding the Age Appropriate Design Code. While the form of the Code and the children's access assessment guidance are matters for the Information Commissioner's Office (ICO) and Ofcom respectively as independent regulators, I would like to take this opportunity to set out in further detail how the Bill will align with the Code to provide consistency for those providers who are in scope of both regimes.

The Data Protection Act considers services to be in scope of the Information Commissioner's Age Appropriate Design Code ('the Code') if they are 'likely to be accessed by children'. While the test in the Bill has been designed to provide more legal certainty and clarity for providers than the test outlined in the Data Protection Act by expanding on when a service will be considered 'likely to be accessed by children', this has been done in a way that is in part informed by the approach taken by the ICO in the Code.

Overall, the two approaches are closely aligned, meaning that there will be a similar effect when implementing both the Bill and the Code in practice. For instance, both tests require providers to consider whether it is possible for children to access the service and whether there are measures in place to prevent children from accessing the service. In addition, both tests require providers to consider whether children already form a *significant* number or proportion of the user base. The word 'significant' here means both a significant number in itself, or in relation to the number of UK-based users on a service. Both tests are also met where children do not form part of the intended user base of a service, but where they are users of a service, and where children are likely to be attracted to use the service. Both tests also require service providers to keep their assessments under review, and consider any emerging evidence that indicates that children are likely to access their service, and comply with either the child safety duties or Code as a result.

Ofcom will be required to produce and publish guidance for providers on undertaking the children's access assessment, which will expand on the Bill's provisions in a similar way to the guidance prepared by the ICO on the Data Protection Act. Ofcom will be required to consult the ICO on its guidance to providers which will further support alignment between the tests in the Bill and the Code for those providers who are in scope of both regimes.

A more detailed comparison of the two approaches can be found in the table below.

Age Appropriate Design Code	Online Safety Bill
The Data Protection Act sets out that the Information Commissioner must prepare a code of practice containing guidance on 'standards of age-appropriate design of relevant information society services which are likely to be accessed by children'.[1] There is no further provision in the legislation about the interpretation of this test, but the Code itself then provides further guidance to providers on when the test of 'likely to be accessed by children' is likely to have been met.[2] This includes the following provisions: ● a service is in scope if it is designed for and aimed specifically at children; ● services which are not specifically aimed or targeted at children but are nonetheless likely to be used by children are in scope; ● for a service to be 'likely' to be accessed, the possibility of this happening needs to be more probable than not. The Code states that this recognises the intention of Parliament to cover services that children use in reality, but does not extend the definition to cover all services that children could possibly access; ● in practice, whether a service is likely to be accessed by children or not is likely to depend on: first, the nature and content of the service and whether that has particular appeal for children; and second, the way in which the service is accessed and any measures put in place to prevent children gaining access;	When designing the Bill, we deliberately sought to align our approach with the Code to ensure consistency across regulation and for providers. The key provisions of the Online Safety Bill are: ● that all providers in scope of Part 3 of the Bill must undertake a children's access assessment; ● to undertake this assessment, a service provider must first determine whether it is possible for children to access the service, or a part of it. They may only conclude that it is not possible for children to access a service, or a part of it, if there are systems or processes in place to prevent children from accessing it, for example age verification or another means of age assurance; ● if it is possible for children to access the service, providers must then determine whether the child user condition is met. This is met if: ○ there is a significant number of children who are users of the service or of that part of it, or ○ the service, or that part of it, is of a kind likely to attract a significant number of users who are children. ● a significant number of children includes a number which is significant in itself, or a significant proportion of the total number of UK-based users on a service; ● whether there are a significant number of children who are users of the service should be drawn on evidence about who

[1] Section 123(1) of the Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/section/123/enacted

[2] Information Commissioner's Age Appropriate Design Code: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/

• if children form a substantive and identifiable user group on an existing service, the Code will apply. In addition to the information included in the Code, the ICO has recently consulted on further guidance for services on applying the test of 'likely to be accessed by children'.[3] While this still remains draft guidance, key provisions include the following: • the code applies both to services that are intended for use by children, and to services that are not aimed at children, but are accessed by a "significant number of children"; • a "significant number of children" means that the number of children accessing or likely to access the service is material, such that the code should be applied; • 'significant' in this context does not mean that a large number of children must be using the service. Rather, it means that there are more than a *de minimis* or insignificant number of children using the service. This low threshold depends on a variety of factors relating to the type of service and how it has been designed; • to decide whether children are likely to access the service providers could take into account a list of non-exhaustive factors; • the list of non-exhaustive factors includes actual evidence or information that a service may have that children are accessing its site; • one example of such evidence is whether the number of UK child users may be considered significant in absolute terms or	actually uses a service, rather than who the intended users of the service are; • providers must make and keep a written record, in an easily understandable form, of every children's access assessment; • all services that assess themselves as likely to be accessed by children will need to conduct a children's risk assessment and put in place systems and processes to protect children from harmful content and activity.

[3] ICO draft guidance on 'likely to be accessed by children' FAQs, list of factors and case studies: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/#FAQs

in relation to the proportion it represents of total UK users of the service or the number of children in the UK. Services should use current UK population information to assess the latter. Sources of evidence may include any age information that services have available, such as information gathered from age profiling tools being used, a service's own research about its users, or information about advertising targeted at children; • other factors that services could take into account include considerations about the types of content, design features and activities in which children are interested, any publicly available research evidence, and whether children are known to like or access similar sites.	