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

18 May 2023

To: All Peers

INT2023/05727/DC

My Lords,

ONLINE SAFETY BILL: FOLLOW-UP TO DEBATE ON DAYS 3–6 OF LORDS COMMITTEE

As promised, I am pleased to follow up on a number of issues raised during the debate on the third, fourth, fifth and sixth days of Committee Stage. As always, I am grateful to everyone who took part in the debates.

DAY THREE

Lord Stevenson of Balmacara requested clarification on the differences between the Online Safety Bill and the Regulation of Investigatory Powers Act 2000 — and the separate purpose of the Investigatory Powers Act 2016 — in relation to access to information in private settings.

During the debate on privacy and encryption, there were requests for clarification on the differences between the oversight regimes for the notices powers under clause 110 of the Online Safety Bill and the notices powers under Part 4 and sections 252 and 253 of the Investigatory Powers Act 2016.

The powers in the Investigatory Powers Act are fundamentally different to the notices power under clause 110 of the Online Safety Bill. As both regimes have different effects, they also have differing safeguards. The Investigatory Powers Act gives the Secretary of State (usually the Home Secretary) powers to require telecommunications operators:

- to retain communications data;
- to provide and maintain technical capabilities enabling them to respond to relevant authorisations or warrants allowing access to communications data or the content of a communications, or to enable equipment interference; or
- to take such specified steps as the Secretary of State considers necessary in the interests of national security.

Notices under the Investigatory Powers Act can only be given where necessary and proportionate to secure the respective capability. All three types of notice are subject to a 'double-lock' (i.e. approval by both the Secretary of State and a Judicial Commissioner) before they can

be given to the operator in question. The Investigatory Powers Act also lays out the factors the Secretary of State must consider when deciding whether to give a notice.

Separate measures exist in Part 3 of the Regulation of Investigatory Powers Act to ensure that the ability of public authorities to protect the public, and the effectiveness of their statutory powers, are not undermined by the use of technologies to protect electronic information. In practice, this can mean requiring an individual to provide the passcode to a device by seeking appropriate permission as specified under Schedule 2 of that Act, e.g. permission granted by a judge, as a result of the data having been obtained under a warrant, or in the exercise of other statutory powers. The Investigatory Powers Act and the Regulation of Investigatory Powers Act therefore provide tools solely for use by law enforcement and intelligence agencies and other specified public authorities.

In contrast, the Online Safety Bill empowers a regulator (Ofcom) to ensure that online services are taking the appropriate steps to keep their own users safe from the most serious harm. There are no powers in the Bill for HM Government to require that it be given access to content on private channels. Instead, the Bill requires companies to implement proportionate systems and processes to tackle illegal content on their platforms.

Ofcom is operationally independent and there are already significant safeguards built into the legislation to govern its use of the notices power in clause 110 of the Bill. Ofcom must consider a wide range of factors, including risk of harm and prevalence of harm, when deciding whether to use its powers. This will help ensure that users' rights are duly protected. The Information Commissioner's Office must be consulted on Ofcom's codes of practice relating to child sexual abuse/exploitation and terrorism content, and guidance on how it proposes to exercise its notices power under clause 110, ensuring that privacy considerations continue to be at the heart of the regime.

Ofcom has the power to draw on expert opinion throughout the notice process using the skilled persons' reports provisions. These were recently amended to allow Ofcom to rely on third-party experts to inspect a regulated service to aid its decision on whether to issue a notice. This independent, expert scrutiny will ensure that Ofcom has a full understanding of relevant factors and technical issues to inform decisions on how best to mitigate child sexual exploitation/abuse or terrorism risks in relation to the regulated service.

For these reasons, we do not consider that further independent oversight of the use of this power is required.

A number of Noble Lords asked about the term 'best endeavours' and how it applies to the notices power. To clarify, 'best endeavours' refers to the process of developing or sourcing new technology when a company is required to by Ofcom under a child sexual abuse/exploitation notice because appropriate or compatible accredited technology is not available for that service.

We have not sought to set out a definition of 'best endeavours' in the legislation to allow for flexibility and proportionality, because what best endeavours might entail will be dependent on the nature of the platform, its resources, and the risk in question. Any steps required under a notice to demonstrate 'best endeavours' must be proportionate; Ofcom will have examined the circumstances and the requirement for a notice on a case-by-case basis before setting out steps the company should take.

Thirdly, I want to clarify an issue raised in the debate regarding whether the power can only be used in relation to illegal content. As I mentioned, there are stringent safeguards in relation to the powers under clause 110. This includes consideration of the prevalence of illegal terrorism and child sexual abuse/exploitation content on a service. This power can only be used where

criminal activity is taking place. It is also worth noting that the power can only be used on private channels to address child sexual abuse/exploitation offences, as the notices for terrorist content can only be used on public channels.

Finally, I wanted to take the opportunity to respond to points made about end-to-end encryption. HM Government has always been clear about the important role strong encryption plays in protecting privacy, personal data, intellectual property, trade secrets, and cyber security. We support the responsible use of encryption where public safety is designed as part of it, and remain concerned where encryption wholly precludes any legal access to content.

The Government believes that technology can support the implementation of end-to-end encryption in such a way that can protect children from abuse online, while respecting users' privacy. We have seen companies develop such solutions for platforms with end-to-end encryption before, and the Government provided investment through the Safety Tech Challenge Fund to demonstrate possible solutions which enable child sexual abuse/exploitation to be tackled by companies in private channels. Where technology which is compatible with a particular service design is available Ofcom should be able to require its use, subject to strict privacy safeguards. Where off-the-shelf solutions in relation to a particular service design are not available, it is right that the Government has led the way in exploring these technologies. We expect the industry to use its extensive expertise and resources to innovate and build robust solutions for individual platforms/services that ensure both privacy and child safety by preventing child abuse content from being freely shared on public and private channels.

Lord Allan of Hallam asked why I described Lord Clement-Jones's proposed amendments to clause 170 as creating a more 'subjective' standard for removal.

Clause 170 sets a specific threshold for providers to make judgements about content. It states that providers' systems and processes for fulfilling their obligations under the Bill should make judgements on the basis of all reasonably available, relevant information about the content. Providers should treat content as illegal content or a fraudulent advertisement where consideration of all the reasonably available, relevant information gives them 'reasonable grounds to infer' that all the necessary elements of the offence are present and that no defence may be successfully relied upon.

'Reasonable grounds to infer' is an objective test because it is founded on the concept of reasonableness. It sets a common bar for all providers. Providers will not be required to treat content as illegal content where, for example, the reasonably available, relevant evidence is only sufficient to give rise to a suspicion that the content may be illegal.

Under Lord Clement-Jones's amendments, providers would be required to treat content as illegal content only where there was 'sufficient evidence' that all the necessary elements of the offence were present and that no defence might be successfully relied upon.

This formulation would not specify the point at which a provider should consider that there is 'sufficient evidence'. Providers would be able to reach different conclusions of what was 'sufficient', each of which would be equally valid, because there is no requirement in the amendment that that determination should be reasonable or otherwise linked to an objective standard. The test would therefore be a subjective one.

This could lead to providers removing too much or too little content under the Bill, for instance if they took the view that 'sufficient evidence' would only be available in cases where a court had ruled that the content amounted to a criminal offence, or if they considered that evidence which gave rise to a mere suspicion of illegality was 'sufficient'. This uncertainty about what level of evidence is 'sufficient' would also pose enforcement challenges for Ofcom.

Lord Allan also asked about jurisdiction, and whether illegal content originating overseas is in scope of the legislation.

As I referred to during the debate on illegal content, the relevant provision in the Bill determining this point is Clause 53(11), which states:

'For the purposes of determining whether content amounts to an offence, no account is to be taken of whether or not anything done in relation to the content takes place in any part of the United Kingdom.'

Companies will therefore be subject to the illegal content duties imposed by the Bill in relation to any content available to UK users on their services which amounts to an offence in the UK. It is irrelevant for these purposes where the person committing the offence is located, or where the elements of the offence are committed.

DAY FOUR

Lord Clement Jones asked for further clarification about the purpose of clause 11(14).

Clause 11 imposes duties on providers in relation to content which is harmful due to its nature, due to the fact of its dissemination, or due to the manner of its dissemination. I can provide reassurance that cumulative risk will be addressed under the safety duties in clause 11(2), which imposes a broader requirement on providers to mitigate and manage the risks of harm to children on their service, including from harm caused through the dissemination of content. This duty applies across all areas of a service, including the way it is operated and used by children as well as content present on the service. The definition of 'harm' set out in clause 205 also clearly recognises that harm can arise from the manner in which content is disseminated.

As part of their child safety risk assessments, providers will need to assess the risk of harm to children from the different ways in which their service can be used, the design and operation of the service, and functionalities which facilitate the presence or dissemination of content that is harmful to children, such as algorithms. Providers will then need to take steps to mitigate and manage the risks of harm to children on their service.

Some provisions in clause 11, however, are only workable in relation to content which is harmful to children where the risk of harm is presented by the nature of the content. Clause 11(14) identifies these provisions to ensure the workability of the clause. It would not be feasible for providers to fulfil the duties at 11(3) and 11(6) relating to primary priority and priority content in relation to content which is only harmful by the fact of its dissemination. It would be wrong to interpret this as meaning that the safety duty as a whole does not apply in relation to content which is harmful due to the fact of its dissemination.

The example I gave during the debate was content discussing a mental health condition such as depression. *Ipso facto*, this content would not be inherently harmful to all children encountering it, but due to the manner of its dissemination it might be harmful to a particular targeted child — for example, where recommendations were made to that child repeatedly through the use of algorithms. It would neither be workable nor proportionate for a provider to prevent or protect all children from encountering singular instances of this type of content, which is why clause 11(14) is needed.

Lord Knight of Weymouth asked for confirmation of whether the child safety duties apply regardless of whether a virtual private network (VPN) has been used to access the

systems and the content, and whether it was technically possible for providers to detect the use of VPNs.

While the development of new VPN technologies is evolving, I can confirm that it is currently technically possible for website operators to detect and block VPN users. As I indicated in my closing speech, service providers are already required to consider how safety measures could be circumvented, and to take steps to prevent that. This is set out clearly in the children's risk assessment and safety duties. Under the duty at clause 10(6)(f), all providers of user-to-user services must consider the different ways in which the service is used and the impact of such use on the level of risk.

The use of VPNs would be one factor which could affect risk levels. Service providers must also ensure that they are effectively mitigating and managing risks they identify, as required by clause 11(2). Ofcom will set out steps that providers can take to meet the child safety duties in codes of practice, and under paragraph 2(c) of Schedule 4 they must ensure that the measures described in the code of practice are technically feasible. These could include recommendations in relation to VPNs.

Baroness Harding of Winscombe asked whether Ofcom has the resources to manage companies taking alternative approaches to those measures in the Codes of Practice.

Firstly, it is important to say that in most circumstances we expect companies to take the measures outlined in Ofcom's codes of practice as the easiest route to compliance. It is, however, important that there be the option for companies to pursue alternative measures provided they still satisfy the duties, in order to ensure that innovation in this dynamic sector is not hindered and that new methods to protect users from evolving threats can be developed.

HM Government has worked closely with Ofcom to develop this model. Following pre-legislative scrutiny of the Bill, we strengthened the provisions which require services to document and justify fully any alternative measures taken, in order to make it easier for Ofcom to evaluate the steps taken by a given service and aid enforcement action. As a result, we are confident that Ofcom has the resources to manage platforms which choose to take alternative measures.

DAY FIVE

Baroness Kidron asked for clarification of the user verification provisions in relation to Meta.

Lady Kidron asked whether the 'Meta Verified' product would qualify as user verification under the terms of the Bill. She and Lady Merron also raised the affordability of verification services.

As I said in the debate, clause 57 specifically sets out that services will be required to offer all adult users the option to verify their identity. The Bill does not specify whether or not a provider can charge for a verification service. Providers will, however, need to fulfil the requirements in the Bill that verification tools or features must be offered to all adult users and that the verification process must be explained in a clear and accessible way.

In addition, Ofcom will be required to produce and publish guidance on user identity verification, which is intended to assist providers in complying with these duties. When creating this guidance, Ofcom will have to consult groups which represent the interests of vulnerable adult users. It must also have regard to the desirability of ensuring that providers of Category 1 services offer forms of identity verification that are likely to be available to vulnerable adult users.

Further clarification on the provisions of the Bill in relation to Article 8 of the European Convention on Human Rights.

Amendment 60 (tabled by Lord Clement-Jones) and Amendment 88 (tabled by Lord Stevenson of Balmacara) explore whether references to privacy law in Clauses 18 and 28 of the Bill include Article 8 of the European Convention on Human Rights (ECHR). Given the technical nature of this subject, I felt it might be helpful to provide further clarification in writing.

Clauses 18 and 28 of the Bill require all user-to-user and search services in scope of the Bill to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy which is relevant to the use or operation of the service when deciding on, and implementing, safety measures and policies. As Article 8 of the ECHR, along with other Convention rights, has been given statutory footing in UK law by the Human Rights Act 1998, this would already be covered by the Bill as drafted as a 'statutory provision'. Providers will also need to have regard to privacy-specific legislation such as the UK General Data Protection Regulation, which ensures that people's privacy rights and personal data are adequately protected.

Ofcom will be required to design codes of practice to be compatible with protecting the privacy of users, and will need to ensure that appropriate safeguards are in place to protect users' privacy. Providers will be treated as complying with their duties to have particular regard to users' privacy if they take the recommended measures that Ofcom sets out in the codes, or alternative steps which have the same effect (see clauses 44(2)(b) and (3)(b)).

Ofcom will be required to consult the Information Commissioner's Office in relation to its codes of practice and when issuing guidance on provisions which could have privacy implications. More generally, we expect Ofcom and the Information Commissioner's Office to work closely together to ensure that services have appropriate privacy safeguards in place.

As a public body, Ofcom is bound by the Human Rights Act 1998. This means that Ofcom has an obligation not to act in a way which is incompatible with the Article 8 right to privacy when carrying out its duties, for which it can be held to account. This will be particularly important when the regulator develops codes of practice and makes enforcement decisions. Ofcom will not be able to put in place and enforce measures which do not comply with Article 8 of the ECHR.

DAY SIX

Baroness Kidron asked how many school children are enrolled in computing classes.

The teaching of computing, which encompasses computer science, ICT and digital literacy, is compulsory in the national curriculum (which applies to all Key Stages, excluding those aged 16 and above) for local authority maintained schools in England. Academies and free schools must teach a broad and balanced curriculum and may use the national curriculum as an exemplar.

Computer science, which is a relatively new subject at GCSE level, saw a rapid increase in pupil entries during its first six years. Pupil entries in England have risen from 4,021 in 2013 to 78,450 in 2022. This accounted for around 12 per cent of the Key Stage 4 cohort in 2022. A Level computer science pupil entries have also increased each year since its introduction in 2013. There were 3,399 entries in 2013, rising to 12,841 in 2021 and 15,000 entries in 2022.

Digital literacy equips pupils with the knowledge, understanding, and skills to use information and communication technology creatively and purposefully. As I highlighted in the debate, however, computing is not the only subject in which media literacy and critical thinking skills are taught in schools.

Citizenship education is compulsory in local authority maintained secondary schools as part of the national curriculum for Key Stages 3 and 4. Primary schools can choose to teach citizenship, using non-statutory programmes of study. As part of this subject, pupils are taught about critical thinking in relation to the proper functioning of a democracy. They learn to distinguish fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. In subjects such as History and English, and the Arts, pupils learn to ask questions about information, think critically and weigh-up arguments - all of which are important media literacy skills.

Baroness Morgan of Cotes asked how transparency reporting, user reporting, and complaint duties will apply in relation to fraudulent advertisements.

In relation to transparency reporting, Ofcom can already require information about how companies are complying with their fraudulent advertising duties through transparency reports. Paragraph 9 in Schedule 8 sets out that Ofcom can require information about the measures taken or in use by a provider to comply with specific duties, including in relation to fraudulent advertising. Further to this, Ofcom will have the power to require any information that it requires from companies about fraudulent advertising for the purposes of carrying out its online safety functions.

In relation to the existing duties on user content reporting and complaints procedures, these have been designed for user-generated content and search content and are not easily applicable to paid-for advertising. The duties on reporting and complaints mechanisms require platforms to take action in relation to individual complaints, but many in-scope services do not have control over the paid-for advertising on their services.

In clauses 33 and 34, however, the largest services (Category 1 and 2A services) which have strong levers over paid-for advertising will have to ensure they have systems and processes in place to enable the swift removal of fraudulent advertising where a provider is alerted of its presence.

As I said in the debate, fully addressing the challenges of paid-for advertising is a wider task than is possible through this Bill alone. Through the Online Advertising Programme, we will be delivering a comprehensive review of the regulatory framework in relation to online advertising. The Government consulted on this work last year and aims to publish a response in due course.

I hope these answers resolve the questions which were raised in each of these areas. I look forward to continuing our debate on this important Bill over the coming days.

With best wishes,

Parkinson of Whitley Bay

Lord Parkinson of Whitley Bay
Minister for Arts & Heritage