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

25 July 2023

To: All Peers

INT2023/08093/DC

My Lords,

ONLINE SAFETY BILL: FOLLOW UP TO DEBATE ON DAYS 4 AND 5 OF REPORT

Thank you to all those who took part in the final two days of Report stage on the Online Safety Bill. I am pleased to provide further information below on a number of issues which were raised. The clause numbers in this letter correspond with the bill print as it was debated at Report stage, which was published 22 June 2023.

DAY FOUR

Lord Clement-Jones asked whether there is a duty on domestic digital regulators to collaborate.

There is no general duty for all the UK's digital regulators to collaborate but, where appropriate and proportionate, we have used the Bill to strengthen co-operation between them – for example, by requiring Ofcom to consult the Information Commissioner's Office when developing codes of practice and guidance which could have an impact on privacy. In addition, Ofcom has a legislative basis to share information with other UK regulators under the Communications Act 2003. Section 393 of that Act sets out clear gateways for the disclosure of information with relevant persons, for example other UK regulators. These can be expanded via an order made by the Secretary of State. For example, the Information Commissioner was added via a Communications Act 2003 (Disclosure of Information) Order.

Ofcom has strong existing relationships with other regulators, including through the Digital Regulation Co-operation Forum. The work of the Forum demonstrates the progress that can be made through voluntary co-operation allowing for an agile response, which is important given the evolving nature of digital technologies. Creating overarching statutory requirements to collaborate would risk adding burdens and complexity to the regulatory landscape at a time when regulatory regimes and remits are rapidly evolving.

Baroness Finlay of Llandaff requested further detail on what she considered to be unregulated services under the Bill, and how the Bill would cover machine-generated content which exhibits problematic behaviours.

The Bill will apply to user-to-user services, search services, and services which publish or display pornographic content.

The Bill is focused on user-to-user and search services as there is significant evidence to support the case for regulation, based on risk of harm to users and the current lack of regulatory or other routes of accountability. The hosting, sharing and discovery of user-generated content and activity give rise to a range of online harms, which is why we have focused on these services.

The Bill ensures that machine-generated content on user-to-user services created by automated tools or machine 'bots' will be regulated where appropriate, as per clause 49(4). Machine-generated content will be regulated *unless* the bot or automated tool producing the content is controlled by the provider of the service.

Providers will therefore be required to design their systems and processes to prevent and remove priority illegal content (for example, child sexual abuse and exploitation material or so-called 'revenge pornography'), regardless of whether it appears online because of a human user, a bot, or AI tools. Providers will also need to remove any other illegal machine-generated content when it has been flagged to them. This will protect users from the most harmful material online.

The Bill does not regulate content published by the providers of user-to-user services themselves. Providers are already liable for the content they publish on their service themselves and the criminal law is the most appropriate mechanism for dealing with those which publish illegal provider content. The one exception to this in the Bill, as I set out, is pornography, which is regulated by Part 5 of the Bill. Services which publish or display provider pornographic content are required to use age verification or age estimation to ensure that children cannot normally encounter this content. This is an access requirement and does not alter the potential for criminal liability which already exists for material they publish.

Lord Stevenson of Balmacara asked about the process for legislative consent in the devolved legislatures.

Offences made by devolved authorities which are not listed in Schedules 5, 6, or 7 will only be a 'relevant offence' for the purposes of the Bill if they are of one of the two types of legislation set out in clause 53(5)(c) (iii) or (iv). Other legislation made by the devolved authorities which does not fit within those categories and is not listed in Schedules 5, 6, or 7 will not be captured by the regulatory framework. This is to ensure that it is as simple as possible for services to comply with the framework, without having to consult various different statute books.

Instead, an offence made by a devolved authority will automatically be in scope of the regime if it is of one of the two types set out in those clauses – that is, if it is either:

- under 53(5)(c)(iii) an Order, Rules, or Regulations made jointly with the Secretary of State or another Minister of the Crown; or
- under 53(5)(c)(iv) a piece of devolved subordinate legislation made by a devolved authority with the consent of the Secretary of State or another Minister of the Crown.

53(5)(c)(iv) is designed to cover relatively rare cases, relating to subordinate devolved legislation, which may only be made by the devolved authority with the consent of the Secretary of State. Examples of how this type of legislation operates are sections 8 and 9 of the Electronic Communications Act 2000 and SSI 2008/92 (relating to pension schemes).

Crucially, to allay Lord Stevenson's chief concern, this clause of the Bill is not introducing any new consent requirements. The consent requirements will be set out in the parent legislation which gives the power for the particular piece of relevant subordinate devolved legislation to be made. There is therefore no further requirement for consent to be within scope of the definition of 'relevant offence' for the Bill.

Baroness Fraser of Craigmaddie raised concerns that there is currently no equivalent in the Online Safety Bill to the Communications Act 2003 which requires Ofcom to report in a nation-by-nation manner.

The overarching principle duty on Ofcom under section 3(1) of the Communications Act already requires Ofcom, when carrying out its functions, to further the interests of all members of the public in the UK in relation to communications matters. Section 3(4)(l) requires Ofcom to have regard in performing its duties, as relevant in the circumstances, to the 'different interests of persons living in different parts of the UK'.

These general duties are being expanded under the Online Safety Bill to extend to Ofcom's new online safety functions: Ofcom would therefore have to take account of these principal duties when fulfilling its duties under the online safety regulatory framework.

Where Ofcom is currently required to produce reports in other sectors that it regulates, there are cases where the legislative reporting requirements do not require Ofcom to report individually on each nation of the UK, but Ofcom opts to do so proactively, in line with its overarching general duties – for example through its Connected Nations and Media Nations reports.

It is important that Ofcom has the flexibility to prioritise and target its regulatory activities where needed. This includes in relation to its reporting activity, which will shed light on the experiences of users across the UK. However, as I highlighted in the debate, Ofcom has a strong track record of producing data that is representative of people across the whole United Kingdom.

Lord Allan of Hallam and Lord Knight of Weymouth asked whether amendments could be made to Schedule 12 to confer further powers to Ofcom to achieve the policy intent of Government amendment 247A.

Amendment 247A is designed to enhance and complement Ofcom's existing information-gathering powers in clause 91. Schedule 12 is about Ofcom's access to the UK premises of service providers. Amending clause 9 (the information-gathering powers), rather than Schedule 12 therefore better meets the policy intention of making access to such information more efficient for Ofcom and providers. The clause 91 power already applies extraterritorially, and ensures that the clause 92 information notice provisions and safeguards apply to the use of this power. Both the Schedule 12 and the information-gathering provisions are based on existing powers in other UK regulatory frameworks (including in the regulation of financial services and data protection).

Under clause 91, the Bill confers powers on Ofcom to require regulated services to provide it with information related to its regulatory functions. Under the information-gathering powers before the amendment we have made, Ofcom would have been able to require providers to obtain or generate information (for instance by carrying out tests of their systems, processes or features, including algorithms) and then submit the requested information to Ofcom. Government amendment 247A provides a new method for Ofcom to obtain this information which recognises the global nature of regulated services and makes Ofcom's vital information-gathering functions more efficient and fit for the modern age.

Without Government amendment 247A, obtaining such information would likely have required multiple information requests or extensive engagement by Ofcom. This amendment will therefore facilitate Ofcom's viewing of information which is likely to enable it more effectively to design the parameters of a test and thereby issue fewer information notices setting out the requirements of the test. This would limit the risk of confusion or repetition in the process and is likely to be more efficient for both Ofcom and service providers.

Schedule 12 concerns access to physical premises, and it would not be feasible to use these powers in respect of non-UK premises. The safeguards in Schedule 12 which are aimed at physical entry to premises would not be appropriate for the new power. Should a provider refuse to comply with the Schedule 12 powers of entry and inspection without a warrant, Ofcom would be able to apply for a warrant in order to exercise further powers such as the seizure of documents and equipment. This would not be relevant or necessary if Ofcom were requiring remote access in order to observe tests, which is far less intrusive than the powers exercisable under warrant which are designed for instances of non-compliance.

However, the power to supervise and observe tests is subject to a number of safeguards through the provisions set out in clauses 91, 92 and elsewhere in the Bill. Clause 91(3) confers on Ofcom a legal duty to exercise the powers to supervise and observe tests in a way that is proportionate, ensuring that undue burdens are not placed on businesses. Ofcom would be unable to exercise this power unless it is justified.

The power is limited to viewing, meaning that Ofcom will be unable to interfere with or access the service for any other purpose when exercising this power. The tests that Ofcom anticipates observing involve the use of a test dataset to see how the algorithmic system works. It would not involve observing the live provision of the service or live user data. Assessing systems, processes, features and functionalities is the focus of these powers – as such, individual user data and content are unlikely to be the focus.

Ofcom is subject to strict confidentiality requirements under section 393 of the Communications Act, meaning Ofcom will not be able to disclose this information without the provider's consent unless a specific statutory exception applies. Ofcom would also be required to comply with obligations under data protection law and users' rights to privacy under the Human Rights Act when considering if it would be proportionate to access private user information. In addition, under clause 91(7) Ofcom is prohibited from requiring the provision of legally privileged material.

As I made clear in the debate, a provider would have a right to bring a legal challenge against Ofcom if it considered that a particular exercise of the information-gathering power was unlawful.

Lord Allan asked for assurances about the process for issuing information notices and whether a provider can challenge a notice before it is issued on the grounds of a security risk, rather than having to seek judicial review of a decision.

Ofcom expects to engage with providers as appropriate about how to obtain the information it needs to carry out its functions. Ofcom's current practice is to issue statutory information requests in draft form in order to give providers the opportunity to identify potential issues that need to be addressed before issuing a final information notice. This could include consideration of any security risks that providers identify.

Due to the requirement on Ofcom to exercise its information-gathering powers proportionately, Ofcom would need to consider if there was a less onerous method of obtaining the necessary information before deciding whether to exercise the power remotely to observe tests of systems, processes or features, including functionalities and algorithms. Ofcom may, for example, consider using its other powers, such as an audit, or a skilled person's report, but we anticipate that, in particular for smaller services, those options could be more burdensome than Ofcom observing specific tests. Ofcom will seek to ensure it is able to obtain the information it needs to discharge its functions in a way that mitigates security risks and is least burdensome and disruptive for providers.

Ofcom would be required under clause 92 to specify (among other things) the information to be provided, setting the parameters of access, and why Ofcom requires the information, explaining the link between the requested information and Ofcom's online safety functions. If Ofcom issues an information request, and companies still have genuine concerns that what Ofcom is asking for is inappropriate or poses a significant security threat, following further engagement on the issue Ofcom may cancel an information notice by notice to the person to whom it was given under clause 92(7).

As noted in the debate, a provider would have a right to bring a legal challenge if it considered that a particular exercise of the power to remotely supervise and observe tests was disproportionate and consequently unlawful.

Regarding Lord Allan's concern that services should be able to challenge information requests first and have those challenges decided before they are required to comply with the notices, it is possible for a service to apply to the court for interim relief which suspends the firm's obligation to comply with Ofcom's notice until after the court has decided their judicial review. The Administrative Court in England and Wales has existing processes to decide interim relief applications on an urgent basis.

Lord Clement-Jones asked which media literacy power would be invoked in the event of the outbreak of disease or riots.

Lord Clement-Jones asked about the power for the Secretary of State to direct Ofcom to give priority to specific objectives when exercising its media literacy functions in exceptional circumstances.

The Secretary of State's direction would set objectives to which Ofcom must give priority when exercising its media literacy functions. On receipt of the direction, Ofcom would need to consider the best way to use its media literacy functions to address the threat caused by the exceptional circumstances.

Lord Clement-Jones is right to point out that Ofcom has a number of media literacy functions under section 11 of the Communications Act 2003. Which of these functions would be best suited to address the objective set in the direction would depend on the specific circumstances. It would not be possible to stipulate which specific objective or objectives that might be, given the nature of the threat may change and given that different circumstances may require different objectives.

By enabling the Government to bolster Ofcom's work on media literacy in this limited way during crises, however, we believe the power provided in clause 158 will further ensure people are equipped to protect themselves and others from harmful content, including mis- and disinformation, at critical times.

DAY FIVE

Lord Allan asked for further clarification on the impact of the Bill's funding regime on services of various sizes, needs, and revenue sources.

When calculating fees, the Bill allows for Ofcom to consider not only a provider's qualifying worldwide revenue but also other factors Ofcom considers appropriate. Ofcom is thus able to make different provisions in relation to different kinds of regulated services (clause 79(5)), such as those mentioned by Lord Allan.

The Bill states that fee calculation must be justified and proportionate (clause 79(2)(b)). As part of fulfilling this obligation, Ofcom will be holding a consultation to determine the most appropriate way to calculate fees. Any additional metrics used to calculate fees alongside qualifying worldwide revenue will be laid out in Ofcom's statement of principles, to be published before the first charging year (clause 79). The Government must issue guidance to Ofcom (clause 78) about the principles to be included in this statement.

Baroness Fox of Buckley requested further clarification about the impact of technology notices on encryption. Lord Stevenson asked why there is no reassurance in the Bill that these powers will not involve Ofcom reading private messages or general monitoring.

During the debate on private channels, Baroness Fox requested further clarification that Ofcom's power to issue a notice under clause 111 will not inadvertently involve the breaking of encryption. Lord Stevenson also asked for clarity on why it cannot be made clear on the face of the Bill that Ofcom will not require general monitoring.

The Government has engaged extensively with industry and technical experts throughout the policy development process. The Bill does not require companies to break or weaken encryption – and we have built in strong safeguards to ensure that users' privacy is protected. Ofcom can only require the use of technology on an end-to-end encrypted service when it is technically feasible and has been assessed as meeting minimum standards of accuracy in detecting only child sexual abuse and exploitation content. Ofcom is also required to comply with existing data protection legislation when issuing a clause 111 notice and, as a public body, is bound through the Human Rights Act 1998 by the European Convention on Human Rights, including Articles 8 and 10. When deciding whether to issue a notice, Ofcom will work closely with a service to help identify reasonable, technically feasible solutions to address the child sexual abuse and exploitation risk, including drawing on evidence from the skilled person's report.

If appropriate technology does not exist which meets these requirements, Ofcom cannot require its use. That is why the powers include the ability for Ofcom to require companies to make best endeavours to develop or source a solution. It is right that Ofcom should be able to require technology companies to use their considerable resources and expertise to develop the best possible protections for children in encrypted environments. We recognise that the types of technology a company can use will depend on the nature of its service, including its size, design, and functionalities. Technologies which may be suitable for one service may not be compatible with the design of another.

An example given by parliamentarians of a technique that could be used is client-side scanning, and concerns have been raised that this would weaken encryption. Client-side scanning would allow companies to process the messaging content on a users' device, in order to identify whether the content is child sexual abuse before it enters the end-to-end encrypted environment. Ofcom will make an informed decision on a case-by-case basis as to what technology (if any) it requires under a notice. We cannot pre-empt this decision-making or which technology will be accredited. However, if such technology meets standards for accreditation and complies with data protection legislation, in particular the privacy requirement of Article 8, Ofcom could require its use through a notice under clause 111.

The Bill also does not give Ofcom or the Government any powers to monitor users' private messages. Under clause 59, there is a requirement for companies to report child sexual abuse and exploitation content to the National Crime Agency (NCA). The NCA will only receive and process information provided to it by the company: the Bill does not permit law enforcement agencies to access information held on platforms, including access to private channels. Nor does the Bill introduce or require 'routine scanning' of private communications or the general monitoring of all content. This is not the purpose of this legislation. The regime is based on requiring companies to put in place systems and processes to manage the risks of illegal and harmful content on their platform and there are clear and strong safeguards for privacy which will ensure that users' rights are protected.

Setting out clear and specific safeguards on the face of the Bill will be more effective in protecting users' privacy than making reference to general monitoring. 'General monitoring' is not a clearly defined concept. It is an EU law term which refers to the generalised monitoring of user activity online, although its parameters are not clearly defined in UK or EU law. Including references to it in the Online Safety Bill would cause a lack of clarity and create uncertainty over what does and does not constitute 'general monitoring' which would impede providers' ability to understand the extent of Ofcom's powers and on Ofcom's ability to regulate this vital area effectively.

Lord Weir of Ballyholme asked if Ofcom has the power to act immediately by applying the interim service restrictions when the nature and severity of the content demands.

When speaking to his proposed amendment, Lord Weir reiterated the importance of prompt enforcement action to prevent children from being exposed to harmful content. Lord Weir sought reassurance that Ofcom will have the power to act immediately by applying for interim service restrictions when the nature and severity of the content demands it.

Ofcom has a range of enforcement mechanisms available to it and in some serious cases it will be possible for Ofcom to act swiftly to impose business disruption measures. Interim service restriction orders are amongst the strongest of the enforcement powers in the Bill, and as such will not be used lightly. The same applies with access restriction orders and interim access restriction orders.

Ofcom will have the discretion to use its range of enforcement powers as it considers appropriate on a case-by-case basis. It is important that Ofcom has the discretion to use the suite of powers as it sees fit, to ensure that compliance is enforced effectively and proportionately.

Where proportionate, Ofcom may apply to the court for an interim service and/or access restriction order to be put in place when it is likely that the provider is failing to comply with an enforceable requirement (including the duties in clauses 11 and 72) and there is such a risk of harm that it would not be appropriate to wait to apply for a 'full' access or service restriction order. These orders provide an expedited route to securing a temporary service or access restriction order where needed to protect users from harm.

Baroness Benjamin asked whether Ofcom would be able to enforce compliance on a wide scale, and for reassurance that this would not expose Ofcom to judicial review.

During Committee stage, Lord Bethell proposed an amendment which intended to make explicit on the face of the Bill that Ofcom can seek a court order which would require one or more third-party ancillary service provider(s) to withdraw their services from multiple non-compliant regulated operators, with one application via a schedule of relevant operators rather than relying on Civil Procedure Rules for such an option.

Our position at that time, which remains the same, is that such a measure would not significantly revise Ofcom's powers, as the Civil Procedure Rules already permit that a single claim form may be used to start all claims which can be conveniently disposed of in the same proceedings. The Rules permit any number of claimants or defendants and any number of claims to be covered by one claim form. The overriding objective of the Rules is that cases are dealt with justly and proportionately.

I am grateful to all Noble Lords who spoke in Committee and on Report, and who have devoted many hours of careful scrutiny to this important Bill — it has been strengthened by it.

I am a placing a copy of this letter in the House library.

With best wishes,

Lord Parkinson of Whitley Bay
Minister for Arts & Heritage