Department for Digital, Culture, Media & Sport

Chris Philp MP
Parliamentary Under Secretary of State for Tech and the Digital Economy
4th Floor
100 Parliament Street
London SW1A 2BQ

E: enquiries@dcms.gov.uk

www.gov.uk/dcms

Written evidence submitted by Under Secretary of State, Chris Philp MP, Minister for Tech and the Digital Economy (OSB0243)

Damian Collins MP
Chair
Joint Select Committee
jconlinesafetybill@parliament.uk

26 November 2021
MC2021/20438/DC

Dear Damian,

Thank you for your letter following the evidence session on 4 November. We were grateful for the opportunity to set out how the Bill will achieve the government's aim of making the UK the safest place in the world to be online, particularly for children. I am looking forward to seeing the recommendations that the Joint Committee put forward on the Bill, and as we said at the session will be considering those very seriously to ensure that this important legislation is as effective as possible.

I have answered each of your questions below in turn.

Scope

1. **Could you explain in more detail the legal difficulties that you feel mean paid-foradvertising should not be included in the scope of the draft Bill?**

Including all paid-for advertising in the scope of the Bill could pose significant legal drafting and policy challenges.

Firstly, doing so would require a reconsideration of the services in scope of the Bill to holistically tackle harms associated with all advertising. Online advertising involves different companies to those the government is regulating via the Online Safety Bill, including advertisers and advertising intermediaries, who buy and sell online advertising space across the internet. Expanding the Bill to include all aspects of these actors' work risks spreading
Ofcom's resources too thinly.

Secondly, safety duties on user-to-user and search services may not be appropriate, and in some cases not feasible, for application to advertisers given the very different way in which they operate. Advertising actors rely on very different contractual agreements to publish and disseminate content, in comparison to the user-to-user and search services in scope of the Online Safety Bill. A whole new set of duties would be required to comprehensively address therange of actors involved in the advertising

market. While it might be possible to impose advertising-specific duties on companies in scope of the current legislation, we would need to be satisfied that these were indeed feasible, given the complexities of the advertising market.

Including all paid-for advertising in scope of the framework would also preempt the work of the Online Advertising Programme (along with potential future work by the Advertising Standards Agency) and potentially create complex regulation for consumers and businesses, where distinct elements of paid advertising are regulated through a different regime than the rest spending on whether they are online or non-online.

That said, we will consider whether there are specific aspects of online advertising where there is such clear evidence of immediate serious harm being caused that there is a case to act quickly and decisively through this Bill, rather than waiting for the Online Advertising Programme.

2. **What clarity can you give us about what will be defined as "priority" harmful / illegal content for adults and children?**

The Bill enables the Secretary of State to set out priority categories of illegal content in secondary legislation. We are continuing to work on identifying priority harms. Once the list of harms has been agreed, it will be enacted through regulations subject to the affirmative resolution processes.

Although the final list of offences is yet to be confirmed, priority categories of criminal offences are likely to include hate crime, revenge pornography, promoting or facilitating illegal immigration and the sale of illegal drugs and weapons. In selecting the priority offices, the Secretary of State must take into account the criteria set out in Clause 44, which are:

- The prevalence of the offence,
- The level of risk caused to individuals in the UK; and
- The severity of the harm.

Ofcom will also have a duty to research and advise on categories of content that is harmful to children or legal but harmful to adults, and will want to draw on evidence and stakeholder views to do this.

There will be two levels of priority categories of content that is harmful to children. All children must be prevented from encountering primary priority content, which we expect to include pornographic content. Children in age groups judged to be at risk must be protected from priority content, which we expect to include violent content. Overall, we expect the priority harms for children to include:

- Pornography and extreme violence,
- Material which promotes eating disorders or self-harm,
- Hateful speech that does not meet a criminal threshold,
- Age inappropriate activity such as that found on dating sites,
- Cyberbullying; and
- Types of disinformation that may harm individuals

For content that is legal but harmful to adults, there will be a selection of priority harms set in secondary legislation. These must be specifically covered in companies' risk assessments and terms of service. These will be decided following consultation with Ofcom. However we expect this to include (amongst others) types of online abuse such as racism and misogyny and material promoting self-harm and suicide.

3. **How do you respond to the criticism from Google that this is a draft Bill aimed at social**

media, and that the demands it places on search engines are disproportionate?

Search services play a significant role in enabling users, including children, to access harmful content online. There are clear actions that they can take to mitigate the risk of harm to their users. Ofcom will set out the detailed steps search services can take to address illegal contentand protect children in the codes of practice. We would expect the measures taken, which could include downranking harmful content in search results for child users, preventing autocomplete functions from directing children to harmful content, and signposting children to sources of support if they search for harmful content, to be proportionate to the risk of harm tousers.

We recognise that search services differ from other in-scope services. Regulatory expectations for companies operating search engines will be proportionate and tailored to their functions in the online space, and will respect the rights of service providers and publishers to freedom of expression as well as ensuring user access to information. Accordingly, search engines have adifferent set of duties under the new legislation, and specific steps in codes of practice, when compared to user-to-user services.

This is because search services facilitate harm in a different way to user-to-user services with their role focussed on organising search results. Harm manifests in users being directed towards harmful content through the search service. Search services may also facilitate harm through "predictive search" functionalities which may inadvertently lead users to discover harmful content. As a result, the duties on search services are focussed on minimising the presentation of harmful content to users through search engines functionalities rather than on the content contained in search results itself.

4. **In what circumstances might you use the power to exempt service providers under the provision in Clause 3(8)? What governance would be in place to ensurethat this power was used fairly and consistently?**

The regulatory framework provides the Secretary of State with the power to make regulations to exempt additional user-to-user services or search services if the Secretary of State considers that the risk of harm to UK users presented by those services is low. Such categories could be based, for example, on the presence of only specific limited functionalities on a service. This power will allow the regulatory framework to keep pace with technological and behavioural changes and to ensure that an excessive burden is not placed on businesses.
Regulations made under this power are subject to the affirmative resolution procedure, which requires the approval of both Houses of Parliament.

5. **Can you give us more guidance on how the categorisation for Category 2B will be decided? Will there be a threshold below which companies will not be regulated atall?**

The new regulatory framework will apply to all search services and all companies that allowusers to post content online or to interact with each other which have links with the UK (as defined in Clause 3). Ofcom, however, will take a risk-based, targeted and proportionate approach to oversight and enforcement.

Companies designated as Category 2A (search services) or 2B (user-to-user services) will need to produce transparency reports in addition to compliance with the duties which fall on all in-scope services. The Secretary of State will have the power to set thresholds to determine which services fall into Categories 2A and 2B. For Category 2B services (user-to-user services), the conditions will be based on the number of users, functionalities and any other factors the Secretary of State considers

relevant.

All in-scope companies will be subject to regulation in relation to illegal content, and all in- scope companies likely to be accessed by children will be regulated (i.e. there is no threshold for these matters). Category 1 companies are subject to the regulation around "legal but harmful" content and regulation regarding transparency and considering content of democratic importance and journalistic content. Category 2A and 2B companies are those not in Category 1 byt who are subject to Transparency requirements as set out above.

6. **How will you ensure that the Bill places an appropriate and proportionate reporting burden on i) smaller but high-risk providers and ii) lower risk or start-upproviders?**

Our intention is to deliver a future-proof, proportionate and effective transparency reporting framework which reflects the diversity of services in scope of the online harms regime.

Not all companies in scope of the new framework will be required to produce transparency reports, which means that the lowest risk providers will not face undue burdens. Companies whose services are designated as Category 1 services will be required to report, as will services which meet the additional thresholds for Category 2A and 2B services, that the Secretary of State will have the power to set. This will ensure that the regime is flexible and that smaller high-risk providers can be brought into scope of reporting requirements if necessary.

Additionally, the reporting requirements will not look the same for all companies in scope of the transparency reporting obligations. Clause 49(5) sets out various factors that Ofcom must take into account when deciding which types of information to require from companies. These include the service provider's capacity to produce information, the type of service and the functionalities the service offers, the number of UK users of the service and the proportion of UK users who are children. This will help ensure that the transparency framework reflects the diversity of services in scope.

Ultimately, it will be for the regulator to decide what companies will need to include in their transparency reports. The regulator will consult with a range of stakeholders, including in-scope companies, and will be required to publish guidance on the approach it will take to determine the specific information service providers will need to include.

7. **Given that children are the first order of importance for the government and it wishes to bring pornography sites into scope, can you explain why businesses who already have to do a children's data protection risk assessment (including pornography companies) under the AADC should not be required to check for safety duties in the Bill?**

We want the Bill to make a real difference to children's safety online, and to do so the requirements imposed by the Bill must be targeted and proportionate for businesses and Ofcom. The legislation has been designed to bring into scope user-to-user and search services, which pose the greatest risk of harm to users and where there is currently limited regulatory oversight. Where an in-scope service has, or may appeal to, a significant number or proportion of child users, it will need to provide additional protections for children.

As the Information Commissioner has set out in the Age Appropriate Design Code, if a service is one that children should not be using, such as an adult only, restricted, or otherwise child- inappropriate service, the service's focus should be on how to prevent children's access to it (in which case the Code does not apply), rather than undertaking a data protection impact assessment and making the service

child-friendly. The regulatory framework will cover many ofthe most visited pornography sites, social media, video sharing platforms, forums and search

engines, thereby capturing sites through which a large proportion of children access pornography. Under our online safety proposals, we expect companies to use age verification technologies to prevent children from accessing services which pose the highest risk of harm to children, such as online pornography sites which host user-generated content.

We recognise the concerns that have been raised about protecting children from online pornography on services which do not currently fall within the scope of the Bill. I am grateful for the Committee's work on this issue and as I mentioned during the evidence session, I am exploring ways to provide wider protections for children from accessing all forms of online pornography through the Bill.

8. **It is not clear that the Bill will not offer refuge from the AADC for companies arguing that they are out of scope of the Online Safety Bill for issues of self-harm, diets and other detrimental material. Can you confirm that this is not the case and how that will be clearly stated in the Bill?**

Under the Online Safety Bill, in-scope services which have, or are likely to appeal to, a significant number of child users will have to provide a higher level of protection for children or face tough enforcement action. Where there is user-generated content related to self-harm, diets or other detrimental material which is harmful to children, the regulatory framework will require these services to protect children from that content.

The Bill will not affect whether a service is in scope of the Age Appropriate Design Code, which sets out standards for protecting children's personal data required under existing data protection legislation. We have aligned our approach with the Code (which requires companies to apply the Code's standards where they have assessed that children are 'likely to access' their service) to provide consistency for companies which may be required to comply with both the Code and the child safety duties in the Online Safety legislation.

9. **Why is the tier system banded by size rather than risk, when there is considerable evidence that very small companies can create enormous risks?**

Risk is built into the tiered approach of the Bill. The draft Bill sets out that platforms with the largest reach that pose the greatest risk of harm to users will have additional duties on them, including legal requirements to take action with regard to content that is legal but harmful to adults.

Smaller companies will be subject to the general duties regarding illegal content, and where the service is likely to be accessed by a child, content that is harmful to children. The approach to content that is legal but harmful to adults has been designed to protect freedom of expression. It requires that the largest and riskiest platforms set out whether and how such content is dealt with on their service. This ensures that users of these platforms know what to expect on the service and what is and isn't allowed. If users want to seek out legal but harmful content on other platforms, then they should be able to do so.

10. **If Ofcom will not take an individual complaint, and a company either fails or refuses to support an individual user, what routes does that user have once all the internal processes of the company have been used, in particular if that user is a child?**

It is important that all users, including children, can complain and seek action both if they encounter harmful content on a regulated service, and if they think that a service has treated them unfairly. All companies in scope of the new regulations will have a specific legal duty to have effective and accessible user reporting and redress mechanisms, and Ofcom's codes of

practice will set expectations for these mechanisms. Companies must also ensure these mechanisms can be accessed by people who are not users but who either are targeted by the content or who are acting on behalf of others who require assistance. For example, parents must be able to report instances of their child encountering harmful content. If platforms don't comply with their duties to put in place effective and accessible user reporting and redress mechanisms, Ofcom will be able to take enforcement action and fine the relevant company upto £18 million or 10% of their global annual revenue. The intention is to use these regulations to force companies to set up proper systems themselves.

Although Ofcom will not investigate or arbitrate on individual complaints (owing to the likelihood of becoming overwhelmed by sheer volume), it will be possible for individuals to submit complaints to Ofcom. Ofcom will use aggregate data from user complaints to inform its horizon-scanning, research, supervision and enforcement activity.

Where there is a systemic issue across more than one service or a highly material issue affecting one service, an eligible body representing the interests of UK users of regulated services or members of the public will be able to submit a super-complaint to Ofcom. Ofcom will be required to respond publicly to such complaints within a set time period. Super- complaints will help to ensure that Ofcom is made aware of issues users are facing which maynot otherwise come to Ofcom's attention.

In addition, Ofcom will be under a statutory duty to establish mechanisms for user advocacy foronline harms. This is to ensure that Ofcom is understanding users' experiences, detecting issues early and addressing their concerns.

Duties

11. **Could you explain in more detail the reasons why you feel that an overarching duty of care cannot work in practice?**
    a. **Are these reasons primarily concerned with it being an overarching duty, or being a duty of care?**
    b. **Would having the current duties as subsets of an overarching duty strengthen the Bill overall?**
    c. **Would setting out the objectives of the Bill in the drafting strengthen theduty?**
    d. **How would setting out guiding objectives for the Bill impact the duties ascurrently drafted?**

We do not think it would be possible to draft an overarching all-encompassing 'duty of care' in such a way as to create sufficient legal certainty. We also do not think it would add anything to the existing duties. Simply adding it above the specific duties would create questions about the legal effect of the overarching duty, if it did not add to what companies were already required todo under the specific duties imposed by the Bill. There is some concern that a wholly general duty of care would be hard for Ofcom (or indeed the Courts) to implement due to a potential lack of specificity about what it actually requires companies to do. That is why the more specificduties as set out in the current draft of the Bill have been used.

The Bill creates specific legal risk assessment and safety duties for both user to user and search services for illegal content, content that is harmful to children and, for high-risk, high- reach user-to-user service providers, legal content that is harmful to adults. These duties require companies to identify, understand and assess risks arising from their services and take proportionate action to address them. For illegal content and content that is harmful to childrenthis includes operating their services using proportionate systems and processes to protect users and others affected by content on

their services. For legal but harmful content accessed by adults, companies are required to be transparent about different types of harmful content ontheir services and to do what they say they are going to do to address such content in their terms of service. These detailed duties also provide additional legal certainty for Ofcom's enforcement activity.

We are confident that these duties give effect to the overall objective of tackling online harms and will result in companies taking the type of actions which proponents of an overarching duty of care have envisaged, but in a way which gives users, service providers and Ofcom much more legal certainty than would be possible through a single high-level duty. Given the comprehensive scope of the specific duties, we consider that adding an overarching duty of care would not in practice extend companies' obligations and in fact could lead to confusions about exactly what companies were required to do, undermining the effectiveness of the regime. Having said that, we would welcome the Committee's views on any aspects of online harm which it considers are not captured by the current duties.

We agree that there is a place for objectives in the Bill. This is why Clause 30 sets out online safety objectives for user-to-user services and search services. These objectives will feed through into concrete action by companies via the codes of practice, which must be compatiblewith these objectives.

1. **Why are the safety duties in the draft Bill described as duties of care when theycreate no right of action against individuals or companies and are owed to the regulator and not to users?**

The Bill establishes statutory duties of care, which will be distinct from any duty of care owed by service providers directly to those affected by their activities (for example, in relation to negligence). These statutory duties place clear obligations on service providers and will be enforced by Ofcom as the independent regulator. The safety duties are described as duties of care to reflect the fact that they require service providers to take steps to prevent harm to their users and others who may be adversely affected by the operation of their services. Ofcom will be able to take enforcement action against those companies who fail to discharge their duty ofcare.

The legislation will not affect the existing legal grounds, such as negligence and breach of contract, on which users can bring actions against companies in court. Indeed the new regulatory framework is expected to make legal action against service providers more accessible to users, including by building up legal precedent, giving companies clear legal obligations with regard to the safety of their users and others, and increasing transparency andunderstanding of the online harms landscape.

2. **How compatible is the Bill with the general monitoring of communications regulations previously required under the EU e-commerce directive?**

The government continues to support the protections from liability contained in the Directive for providers of intermediary services, although now the United Kingdom has left the EU it no longer restricts how the government may legislate. For platforms that host user-generated content, there will continue to be a 'notice and take down' regime where the platform must remove illegal content they have knowledge of on notification or risk incurring liability.

However, there is a strong case for mandating the use of technology to identify tightly defined categories of illegal content where there is a threat to national security or the safety of children.

Under the Bill, Ofcom may use the Use of Technology power to compel specific companies to adopt illegal content identification technologies for CSEA and terrorist material. A requirement to use these types of technology may depart from the general monitoring prohibition previously imposed by the e-Commerce Directive. The use of this power is underpinned by safeguards which ensure that any use of automatic tools to identify and remove illegal content are used proportionately to the risk posed by the prevalence of such content on the platform.

3. **The Competition and Markets Authority are concerned that their powers to tackle online consumer harms will be weakened if they are not designated as priority content. What is the Government's view?**

As outlined in the Full Government Response, the new regulatory framework will focus on keeping individuals safe online, and will not tackle consumer protection issues. The CMA has confirmed that they think this issue could be addressed by ensuring the Bill fully excludes consumer protection offences, and we are engaging with the CMA and BEIS to ensure that thisis the case.

Takedown notices

4. **What safeguards should there be to protect intermediaries where a takedown notice is given? E.g. from an action for breach of contract?**

The Online Safety framework focuses on companies having systems and processes in place to protect users from harmful content and behaviour online. There is therefore no procedure for Ofcom to issue 'takedown notices' to regulated services under the Bill. However, as part of itssuite of enforcement powers, Ofcom can apply to the courts for an order to require internet infrastructure providers to block access in the UK to non-compliant services. These sanctions are likely to be used only in exceptional cases as a last resort.

Ofcom must apply to the courts for business disruption sanctions, in light of their serious potential impact on freedom of expression, and also to ensure the proportionality and legality of Ofcom's intervention. Before granting the order, the court must take into account (amongst other things) the rights and obligations of all relevant parties, including the entities on whom the court is considering imposing an order. They will also have the opportunity to make representations to the court so their interests will be taken into account before an order is made.

The Bill also specifically provides that such court orders may include steps that require the termination of an agreement or the prohibition of the performance of such an agreement. Thisaims to make clear any contractual consequences of such orders.

Powers

5. **Why does the Secretary of State have the power to both issue Strategic Priorities,that Ofcom have to have regard to, and guidelines on how they should carry out their tasks?**

The draft Bill clearly sets out the scope of the regime and the remit and powers of Ofcom as regulator. In some areas, the Bill also gives the government certain powers to ensure that the policy intent of the regulatory framework is maintained.

Clause 113 enables the Secretary of State to issue guidance to Ofcom about its exercise of its online harms functions. This power will enable the Secretary of State, if required, to give more certainty to the regulator, companies in scope and other stakeholders on how she expects
Ofcom to carry out its statutory functions. Ofcom must 'have regard' to the guidance.

In contrast, the power set out in Clause 109, for the Secretary of State to publish a statement of strategic priorities in relation to online safety matters, caters for long term changes in the digital and regulatory landscape. A similar power already exists (under section 2A of the Communications Act 2003) for telecommunications, the management of the radio spectrum, and postal services, and a statement in relation to these areas was published in 2019. Under Clause 110, Ofcom must be consulted on a draft of the statement, and the statement must be laid before Parliament for 40 days during which time either House can resolve not to approve it. It is not the government's intention that such a statement will be in place, or be needed, at the outset of the regime.

These powers are part of the overall approach of balancing the need for regulatory independence with appropriate roles for Parliament and government.

6. **The draft Bill proposes to create an advisory committee on disinformation and misinformation. What will be its purpose?**

Ofcom will be required to set up an advisory committee on misinformation and disinformation, which may include rights groups, academics and companies. The role of the advisory committee will be to build understanding and technical knowledge on how to tackle misinformation and disinformation online. Ofcom will determine the terms and the membership of the advisory committee. The advisory committee will publish a report within 18 months after being established, and after that will publish periodic reports so that the committee's work is transparent.

7. **Why does Ofcom have to wait for two years after the draft Bill's passage before a report on independent researcher's access to data? What is the Government's view on creating powers in the draft Bill to allow Ofcom to enforce requirements on companies on access to data for researchers arising out of that review?**

We are supportive of companies improving the ability of independent researchers to access company data, subject to appropriate safeguards. That is why we have tasked Ofcom to produce a report about independent researchers' access to data. This report will look at the opportunities and challenges in this space and will provide key insights about the extent to which people carrying out independent research into online safety are currently able to obtain information, as well as how this might be improved.

Ofcom will not have to wait for two years before they can issue their report. Instead, Ofcom is required to produce the report within two years of the commencement of Clause 101, so they may produce it sooner. Whilst it is important that Ofcom has adequate time to build a detailed understanding of the various considerations associated with researcher access, Ofcom will have flexibility over when they publish the report. Ofcom will consult with academics, the platforms themselves, regulators and civil society to inform its report.

After the publication of the report, Ofcom will be able to prepare guidance about the issues dealt with by the report for providers of regulated services and people carrying out independent research into online safety.

We are confident that this report and any subsequent guidance from Ofcom will help companies and researchers overcome potential challenges associated with researcher access and will encourage safe and responsible sharing of data for research. Ofcom will then be able to require companies to include information about whether, and to what extent, they are providing access to researchers, in their transparency reports. We are considering whether any further measures in this area would be appropriate.

8. **Does Ofcom have power to take action against named directors, on failures otherthan the failure to supply information?**

Ofcom must be able to get the information and data it needs to do its job, so the current draft ofthe Bill includes deferred powers to introduce criminal liability for named senior executives at tech companies who do not ensure that their firm complies with information requests from Ofcom.

The current draft of the Bill provides that these criminal sanctions cannot be brought in for at least two years after the commencement of the relevant provisions of the Bill, and following a review of the operation of the new regulatory framework. The Secretary of State told the Committee that she is looking to bring them in sooner, because of the urgent need for action totackle harms online and hold senior managers to account.

Ofcom can only take action against senior managers on failures to supply information. We have targeted sanctions in this area as it is vital that Ofcom gets the information it needs to regulate the sector. We also expect these criminal sanctions to instill strong engagement andcooperation with the regime among tech executives, and are satisfied that Ofcom's suite of enforcement powers will push strong compliance across the board.

9. **Where in the Bill is a minimum standard set out for risk assessment?**

The Bill makes detailed provision for risk assessments, through duties on Ofcom and specific duties on companies. Clauses 7 and 19 set out what risk assessments companies must carry out, what factors they have to look at, and require companies to take account of the guidance Ofcom will issue about risk assessments as required by Clause 62. We are confident that theseprovisions will ensure that companies prepare risk assessments that are sufficiently rigorous orface enforcement action by Ofcom.

The Bill also sets out comprehensive lists of factors that a company must consider when carrying out its risk assessments. For example, a company must look at the level of risk of every type of priority illegal content being on its services, the level of risk of harm to users andthe nature and severity of each potential harm and the effect of service design and operation on risk levels.

Clause 82 specifies that these risk assessments are requirements which are enforceable by Ofcom. If Ofcom considers that a company has failed to complete a risk assessment in line with these requirements it can issue a confirmation decision under Clause 83 to require the company to re-complete its risk assessment (or aspects of it) to the required standard and/orimpose a fine in respect of the breach.

In line with the risk-based and proportionate approach to regulation, the Bill does not additionally seek to set a specific standard to determine what needs to be done to comply with these obligations. In this case companies will need to refer to the guidance about compliance with their assessment duties which Ofcom is required to publish under Clause 62, which shouldinclude risk profiles to establish the standards expected of them.

Journalism and News Publisher content

10. **We've heard that as journalism is 'perishable' there should be a duty on providers not to censor it, rather than just to reinstate content after appeal, which could take days. Do you agree this protection needs to be strengthened?**

We believe the Bill includes robust protections for news publishers and for journalism.

We have created an explicit exemption for news publishers' content in the Bill. This means that in-scope services will have no new duties with regard to content published by actors that meet the criteria set out in Clause 40. This ensures that regulation does not incentivise the removal of news publisher content, maintaining the status quo with regard to the moderation of news publisher content on in-scope services.

Recognising the importance of UK internet users being able to access journalistic content, the Bill also includes positive measures to protect a broader category of journalism when shared on in-scope services. The Bill requires Category 1 services to safeguard journalistic content. Under these provisions, Category 1 service providers will need to set out policies that balance the special importance of the free expression of journalistic content against other interests or policies which might lead to it being moderated. These policies will need to give a higher degree of protection to journalistic content than to other forms of content.

Platforms will need to implement their journalism policies consistently and they will need to create expedited routes of appeal where journalistic content is moderated. This will afford journalists increased protection and clarity about the treatment of their content, including where appropriate its swift reinstatement, while retaining platforms' discretion to remove journalistic content in circumstances where it poses a real risk of harm to their users.

Ofcom will hold platforms to account against these duties. It will set out steps that platforms should follow to fulfil their duties in codes of practice. This could include guidance on standards (e.g. timescales) that platforms should meet when considering appeals and reinstating journalistic content.

11. **Does the exemption for "news publisher" content mean that this content is not protected by the duties to have regard to the importance of freedom of speech or the journalistic content appeals process? Can you confirm that you are ready to consider a positive requirement that platforms do not take down news publisher content, as opposed to (or as well as) taking them out of scope.**

News publishers' journalistic content is in scope of Category 1 platforms' duties to safeguard journalistic content, as is made clear in Clause 14(8)(a)(i). These include the duty to make a dedicated and expedited complaints procedure available for journalism. Similarly, under Clause 12, all platforms have a duty to pay due regard to users' rights to freedom of expression when implementing safety policies and procedures, and this includes news publishers' rights where they are users of the relevant platform.

We will consider any recommendations that the Committee chooses to make on protections for news publisher content. However, we believe that the protections set out in response to question 21 provide strong protections to a wide range of journalistic content.

'Positive requirements', which actively prevent social media companies from removing any news publisher content, regardless of whether they consider it to comply with their terms of service or to be suitable for their audience, carry significant risk. This approach would constitute a significant interference with private companies' ability to set their own terms and conditions regarding legal content. Moreover, it could create perverse outcomes if companies were prevented from removing this type of content in all circumstances.

It is also important that the Online Safety Bill is viewed in the context of the government's planned pro-competition regime which will set out a new code of conduct between relevant online platforms with strategic market status and companies that rely on them. This will help to rebalance the wider relationship between platforms and news publishers.

12. **What would be the impact of replacing the "democratic content" and "journalistic content" exceptions with a public interest exception, potentially with journalism and democratic content as non-exhaustive qualifying criteria?**

Major tech companies already exercise huge power over what lawful speech is considered acceptable online and this Bill seeks to address that. As such, given the complexities of defining what the 'public interest' is, there may be concerns about requiring private companies to define what types of content are in the public interest. Our existing approach sets out more precisely the types of content that the government believes it is particularly important to protect.

CSEA and Terrorism Content

13. **Ofcom has raised concerns that the threshold that CSEA and/or terrorism content be "prevalent" or "persistently prevalent" on services before a use of technology notice can be issued is too high. Do you share this concern? What solution do you propose?**

We see the power to issue a Use of Technology Notice as an important tool to empower Ofcom to take effective action to drive down the presence of these awful harms on services.

We are working with Ofcom to consider how this policy will work in practice. The use of these powers must be effectively regulated but we agree that Ofcom must be able to use the power when it is necessary to protect users from harm. We are reviewing the language to consider Ofcom's concerns, but we are clear that the safeguards regulating the use of these powers must remain robust. Consideration of this issue is ongoing.

Criminal Liability

14. **We discussed criminal liability for senior managers. Will this still be specifically for failure to comply with an information notice or do you intend to broaden it to include failures to meet other duties?**

Please see the answer above to question 19.

Under the draft Bill, Ofcom would only be able to take action against named senior managers in relation to failures to supply information. We have targeted sanctions in this area as it is vital that Ofcom gets the information it needs to regulate the sector. As set out above, we also expect these criminal sanctions to instill strong engagement and cooperation with the regime among tech execs, and are satisfied that Ofcom's suite of enforcement powers will push strong compliance across the board.

Age Assurance

15. **The idea of 'likely to be accessed' is dependent on trustworthy age assurance, which must be privacy preserving and mandatory - for both the provider and the services that are checking age. How does the government intend to prevent the systematic failure of services to establish age without setting qualitative and mandatory standards?**

It is important that age assurance solutions are effective, robust, privacy preserving and inclusive. Standards are key to this. DCMS is working with the British Standards Institute and the International Organization for Standardization to develop standards for age assurance products.

This Bill is a framework bill that sets out the duties that in-scope companies will need to meet. Ofcom's codes of practice will set out the steps companies can take in satisfying those safety duties.

We expect Ofcom to include in its Codes steps on age assurance. It may also choose to develop a Code on age assurance. Ofcom will have the ability to include in its codes the high level principles that companies should follow when using age assurance, as well as more granular detail such as the specific industry standards companies are expected to adhere to. Companies will need to follow these steps or demonstrate to Ofcom that they are achieving an equal outcome - it is in this way that companies will be required to achieve the industry standard or equal outcome. Ofcom has duties to undertake extensive consultation on their Codes and we expect that Ofcom will consult with standards bodies as part of developing their Code of Practice on age assurance.

For the 'likely to access' assessment, Ofcom will be required to produce and publish guidance for providers of services on how to make an assessment of whether children are likely to access their service. Ofcom will consult with stakeholders in developing this guidance. This guidance will need to cover all aspects of this assessment, including on determining whether measures in place which mean it is not possible for children to access a service are suitably robust. The requirement to undertake, and keep up to date, an accurate assessment about child access is an enforceable requirement. This means Ofcom can investigate and enforce this requirement where appropriate, and in doing so, Ofcom will take into account its guidance.

16. **In our session it was suggested that companies would have to comply with the Act from 'day one'. In the case of age assurance, how will that be possible, without the necessary consultation and drafting of a code of conduct?**

Our intention is to have the regime operational as soon as possible after Royal Assent, whilst ensuring the necessary preparations are completed effectively and services understand what is expected of them, this includes the use of age assurance.

We are already working closely with Ofcom to ensure that the implementation period that will be necessary following passage of the legislation is as short as possible. The Secretary of State and I are keen to expedite implementation for key parts of the Bill, including age assurance. Options are currently being explored for this. The reference to "day one" (or close to day on) related to the commencement of the processes that lead to full implementation.

17. **How will age verification for commercial pornography be implemented since the Bill repeals DEA part 3 and many sites won't be in scope of the OSB regime?**

The Online Safety Bill will protect children from a broader range of harmful content on a wider range of services than the Digital Economy Act. The Digital Economy Act was criticised for notcovering social media companies, where a considerable quantity of pornographic material is accessible, and which research suggests children use to access pornography. The online safety framework will cover many of the most visited pornography sites, social media, video sharing platforms, forums and search engines, thereby capturing sites through which a large proportion of children access pornography.

Under our proposals, we expect companies to use age assurance, including if necessary verification, technologies to prevent children from accessing services which pose the highest risk of harm to children, such as in-scope online pornography sites. Companies would need to put in place these technologies or demonstrate that the approach they are taking delivers the same level of protection for children, or face enforcement action by the regulator.

I am grateful for the Committee's work on this issue and, as the Secretary of State mentioned during the evidence session, we are exploring ways to provide wider protections for children from accessing all online pornography through the Bill, including on sites not currently coveredby the draft Bill.

18. **In the absence of a mandatory code of conduct on age assurance, what mechanism does the Bill provide for taking regulatory action against sites that do not provide it or who have poorly performing age assurance?**

Ofcom will set out in its codes of practice the steps companies need to take to comply with theirduties under the Bill, which will include where the use of age assurance and age verification is recommended to protect children from harm online. Alongside these steps, Ofcom must also include safeguards to protect users from unwarranted infringements of privacy (Clause 31). In doing so we expect Ofcom to consult with the ICO, drawing on their existing expertise to design such safeguards. This builds on service providers' duty to have regard to the importance of protecting users from unwarranted infringements of privacy when carrying out their safety duties (Clauses 12 and 23). Service providers will be taken as complying with their Clause 12 and 23 duties if they follow these safeguards or put in place other measures that meet the same objectives.

We expect Ofcom to develop a code of practice on age assurance. When using age assurance technologies to comply with the safety duties, companies would need to follow the steps in thiscode or demonstrate that the approach they are taking delivers the same outcome.

Companies must either comply with the steps in the codes of practice or take alternative stepsthat fulfil their duties under the Bill. Ofcom can take robust enforcement action where it finds acompany is breaching its duties, including requiring companies to take specific steps to come into compliance and imposing substantial fines. Ofcom are likely to prioritise enforcement action where children's safety has been compromised.

Follow up - codes of practice

Finally, I also committed in the session to following up with further detail on the parliamentaryprocedure surrounding the codes of practice.

As we discussed, the provision of the Bill relating to the Secretary of State's power to direct Ofcom to modify a code of practice is at Clause 33. Under that clause, once Ofcom has modified the relevant code of practice and the Secretary of State is satisfied that no further changes are required, the Secretary of State must then, under subsection (5), lay the modifiedcode in Parliament, together with a document setting out appropriate details about how Ofcom

has modified the code in response to the Secretary of State's direction. Clause 32(3)-(6) then applies: under the procedure set out in these subsections, the modified code will be issued by Ofcom unless either House of Parliament resolves not to approve it during the 40-day period after the code is laid. In order for either House not to approve the relevant code that House would have to agree a motion - or 'prayer' - to reject it within the 40-day period. In the event of such a motion being brought, the relevant House would debate that motion.

I hope these responses address the questions you have raised and we look forward to seeing the Committee's final recommendations.

With best wishes,

Chris Philp MP
Minister for Tech and the Digital Economy

2 December 2021