Ofcom
making communications work
for everyone

Follow-up note for the Joint Committee on the draft Online Safety Bill

Publication date: 19 November 2021

Contents

Section

Overview

This technical note responds to the further questions on the Online Safety Bill which were set out in your letter of 4 November. We address your questions here under the following headings:

1. Coregulation
2. Timing considerations (combines questions from the risk assessment and codes of practice section of your letter)
3. Risk assessments
4. Audit
5. Accountability
6. Use of technology notices
7. One-to-one services
8. Age Appropriate Design Code
9. Age Assurance and Verification

1. Coregulation

1.1 We understand the Committee's interest in our approach to working with regulatory partners and agree that close working with our partners will be vital to ensure a joined-up approach across the digital landscape to address online harms in a consistent way. Through the DRCF and in other forums we are exploring the range of ways we could work with other organisations with relevant expertise and a shared interest for online safety. We are developing strong working relationships with international regulators, Government departments and agencies across the UK with relevant expertise, universities, research bodies and third sector organisations.

1.2 As part of this, we are exploring the merits of formally designating relevant bodies as co-regulators to deliver specific functions under the legislation. There are a few ways in which this can be facilitated by legislation as we have already discussed. This has been achieved in both the VSP and ODPS regimes through an amendment to the Communications Act to provide Ofcom with a specific power to designate another body as the 'appropriate regulatory authority' for either all or some of our functions. However we can also make use of the Deregulation and Contracting Out Act 1994, and whilst this leads to a lengthier process than providing for a direct power in the Online Safety Bill (akin to the one we have for VSPs and ODPS), it still gives us sufficient flexibility to allow for any such relationship that we identify as suitable for delivering specific functions in the online safety regime. We will continue to explore the opportunities for co-regulation, and step up our engagement with relevant bodies, as the specific functions that Ofcom will need to deliver become clearer.

Q1: The ICO has called for regulators in the Digital Regulation Cooperation Forum to have a duty in legislation to pay regard to each other's work. Would Ofcom welcome such a duty?

1.3 We established the Digital Regulation Cooperation Forum (DRCF) in 2020 to make a step change in our joint working with ICO, CMA and now the FCA. Through this forum we provided advice to government on what further statutory mechanisms might be needed to support regulatory cooperation across digital regulation. This evidence was developed in advance of the draft Online Safety Bill and we are now developing our thinking further with ICO and with government as to the precise mechanisms that are needed in this legislation to ensure that Ofcom and ICO can work together effectively where online safety and privacy regulation interact. In particular we need to ensure that we are able to share information as needed, subject to appropriate safeguards, and that we are able to consult the ICO on privacy matters.

Q2: The ICO has been firm in its view that it is the lead regulator for matters relating to privacy and online data protection. Does Ofcom agree that the ICO should take a lead in these matters?

1.4 The draft Online Safety Bill does not require Ofcom to undertake any substantive consideration of whether providers have complied with their data protection obligations or their obligations under PECR. Such issues would rightly sit with the ICO, as the lead regulator for privacy and data protection.

1.5 The draft Online Safety Bill does impose some privacy-related duties on platforms, for instance: all in scope providers will have to have regard to the importance of protecting users from unwarranted infringements of privacy when deciding on and implementing their safety policies and procedures (clauses 12 and 23), and Category 1 providers will have to carry out an impact assessment which considers the impact of these policies and procedures on the protection of users from unwarranted infringements of privacy, and explain publicly the steps they have taken in response to protect their users from infringements of their privacy rights (clause 12). The draft Bill empowers Ofcom to take enforcement action in relation to these privacy-related duties only if platforms do not have the appropriate safeguards or systems and processes in place to meet them. As we explain in more detail below, we will work closely with the ICO where relevant to inform our approach where there might be overlaps with their areas of expertise, and are well used to doing this already.

Q3: Where regulators coregulate in an area relating to the draft Bill with equivalent powers, what processes would be in place to ensure any disagreement between them or problems that arise could be resolved?

1.6 We understand the importance of ensuring there is clarity about where regulatory responsibility lies, both to respect the remit of individual regulators and to ensure that

regulated entities have certainty about whom they are accountable to, and for what. Specifically in relation to this Bill, we are mindful of the potential interactions between online safety, privacy and data protection issues, and there are also potential interactions between a new digital markets regime and the online safety regime. Were any disagreements or problems to arise in the course of carrying out our new regulatory duties, we are confident that the mechanisms we already have in place would allow us to resolve these.

1.7 We are well used to working through areas of overlap with other regulators, and already have a deep working relationship with the ICO and other digital regulators. As set out above we are continuing to develop our thinking as to whether further mechanisms are needed in the online safety regime to facilitate cooperation. We already have in place a number of mechanisms to facilitate close cooperation and to resolve any areas of potential conflict or disagreement. For instance, since 2019 we have had a Memorandum of Understanding with the ICO, which sets out a framework for cooperation and information sharing. We already share information between each other where appropriate to facilitate our respective functions, and have been working closely together to ensure alignment between Ofcom's video-sharing platform regime and the ICO's Age Appropriate Design Code. In line with our establishment of the DRCF, we intend to continue our consultative approach with other regulators in the new regime so that we can benefit from the their experience and expertise in considering related or overlapping issues, and to mitigate the risk of any inconsistencies between regimes (for example, we would want to engage with the ICO to avoid inadvertently recommending something in codes of practice that would risk putting services in breach of their data protection obligations).

1.8 On 2 November 2021 we gave oral evidence to the Lords Communications and Digital Committee, alongside our DRCF partners. We set out that many of the conversations taking place in the DRCF encourage creative tension, and that the DRCF enables us to strike a balance between our respective objectives. Our objectives are not competing, but in talking through issues from our respective areas of focus it can help to encourage outcomes that address them together. For instance, developing solutions that keep children safe while protecting their privacy.

2. Timing considerations

Q4: By what time frame (from Royal Assent) do you expect the first Ofcom risk assessment to be completed?

Q7: By what time frame (from Royal Assent) do you expect to issue the first Codes of Practice?

2.1 We want the online safety regime to be up and running as quickly as possible to make life online safer for UK users. We are also mindful that industry is keen for clarity about what the expectations on them will be. This was also true of the VSP regime, for which we

assumed new duties in November 2020. When we published our final set of guidance for VSPs in October 2021, we were the first regulator in Europe to reach this important milestone.

2.2 We intend to move as quickly as is practical for the online safety regime too, and the preparatory work we have already started is part of this effort. We are continuing with our world-class research, and have already begun establishing relationships with platforms, some of whom we already have a regulatory relationship with under the VSP regime. Through these relationships, we will further deepen our understanding of the systems and processes that would be proportionate and reasonable to expect companies to have in place but also share our early thinking on the expectations we will have of companies so that they can take steps to prepare in advance of our codes of practice and risk assessment being published.

2.3 There is, however, a limit to the work we can do before being granted new powers under the Bill and we also want to avoid pre-empting the parliamentary process. For example, we will need to be clear on what priority offences and categories of legal but harmful content will fall in scope of the regime before we can develop appropriate recommended steps for inclusion in the codes. It is also important to us that moving quickly does not come at the expense of doing the job well, and ensuring that we have all the information and evidence that we need to secure a fully informed and robust approach. In keeping with the approach we take to our existing regulatory duties and in line with the requirements in the draft Bill, we will consult widely and publicly on the development of the online safety regulatory regime, including the relevant codes of practice.

2.4 We will publish a consultation document setting out our proposals on the content of the first codes of practice as soon as possible after Royal Assent, once we have our statutory powers and have obtained the evidence we need to develop our proposals for consultation. We anticipate that it will likely take at least 12 months to prepare the first codes of practice, including consultation, and our ambition would therefore be to submit our first codes of practice to the Secretary of State around 12 to 18 months after Royal Assent.

2.5 We intend to consult on the first Ofcom risk assessment and risk assessment guidance in parallel with our consultation on the first codes of practice and expect to issue a statement finalising our first risk assessment at the same time as we present our first codes of practice to the Secretary of State. The reason for this is that we think it is important to develop the regulatory regime in respect of risk assessments and the safety duties in parallel to ensure that they work together effectively. It will also enable us to move as quickly as possible.

2.6 Finally, we note that the preparatory work we are undertaking is based on the draft Bill published by the Government earlier this year. Significant changes made to the scope of the regime during the parliamentary process could impact this work, and therefore lengthen the process for consulting and issuing our first codes of practice.

3. Risk assessments

Q5: What kind of consequences would there be under the draft Bill for a risk assessment which i) deliberately and ii) recklessly underestimates risk?

3.1 As we have discussed previously, we think it will be key to the success of the regime to ensure that platform risk assessments enable the platform to adequately assess relevant risks and take appropriate steps to address those risks, and that Ofcom is able to take enforcement action where they do not do so. We understand that Government shares our objective, and they have been clear that they want to ensure the drafting of the Bill meets this objective.

3.2 However, as we have set out previously, we think that there are two areas which require further consideration: (1) whether the Bill currently requires providers to meet any particular standard for risk assessments that they can be held to and (2) whether the Bill will enable us to take effective enforcement action where a provider fails to adequately assess and take appropriate steps to address risks.

3.3 In summary, we consider that under the draft Bill we could take enforcement action in circumstances where providers fail to carry out risk assessments at all, or within the required time limits, or fail to address the specified areas. It may be possible to establish a breach where there is clear evidence of a deliberate failure (although evidencing a provider's subjective intention may be challenging in practice). However, we do not think a breach will follow simply because the provider has come to the wrong answer, or has failed to take due care and attention in assessing the risks arising from their service. In these circumstances, enforcement action will therefore be more challenging.

3.4 We have previously explained the potential limitations on our ability to enforce under the safety duties where the deficiency in a platform's systems and processes flows from a deficient risk assessment. To address this, we think Parliament might wish to consider whether it could be helpful to augment the safety duties to provide a direct means of addressing the underlying harm. We suggest looking at augmenting the safety duties, rather than simply the risk assessment duty, because we think it would be better for Ofcom to be able to take enforcement action against providers to secure directly the necessary improvements to inadequate systems and processes, without having to first demonstrate a specific breach of the risk assessment duty and then wait for providers to re-do their risk assessments properly. For example, one option could be to broaden clauses 9(2) and 10(2) to incorporate harms that were reasonably foreseeable to the provider. An alternative might be to clarify that the 9(3) and 10(3) duties applies more broadly than the output of the risk assessment (and amend 9(6) and 10(6) accordingly), although clearly this would have a slightly different effect, given the more specific requirements of 9(3) and 10(3).

3.5 Alongside this proposed change (or if it is not possible to amend the safety duties, then as an alternative), we would suggest that the risk assessment duties could be amended to

incorporate a concept of "adequacy" or "suitability". This may make it easier to enforce where we can demonstrate that the risk assessment is inadequate (including, for example, where we had evidence to suggest that deficiencies in the risk assessment were reckless or deliberate, or the assessment was deficient for any other reason). Finally, it may be possible to introduce the concept of "reasonable foreseeability" into the risk assessment duty, for example by clarifying that references to "risk" or "level of risk" in the definitions of the various risk assessment mean risks or levels of risk that were reasonably foreseeable. This change could also be made in conjunction with the suggested changes to the safety duties.

Q6: How will you ensure that the burdens of i) risk assessments and ii) transparency reports are proportionate for smaller providers?

3.6 Proportionality will be at the core of our approach to the regime. Our expectations for platforms in meeting all their duties will vary depending on a range of factors including the size, resources and risk profile of companies. We would in general expect larger, better resourced and higher risk services to produce more thorough risk assessments and transparency reports.

3.7 Consistent with the provisions of the Draft Bill, we will produce guidance to assist services in undertaking their risk assessments. This will provide further detail on what risk assessment steps we expect services to take and will include guidance on how our expectations as to the level of detail in risk assessments might vary depending on the size, resources and risk profile of the services in question.

3.8 Unlike the risk assessments which are a requirement for all in-scope services, transparency reports are only a requirement for certain services – those falling into categories 1 and 2. These are intended to be the largest and riskiest services. In addition, under the draft Bill, the transparency report is only an annual requirement and Ofcom is not empowered to request more regular transparency reporting from platforms.

3.9 In advance of the implementation of the transparency regime, Ofcom will carry out stakeholder engagement to better understand what providers are already doing to promote transparency and what more they could do once the regime comes into effect. Ofcom will publicly consult on our transparency reporting guidance after Royal Assent (as required under clause 50), thereby giving providers further opportunity to comment on the approach we will take to their annual transparency reports. We also plan to discuss with providers our proposals for what information should be included in a transparency report in a given year, in advance of issuing the final notice that sets out all the information they'll need to include, to the extent that this would evolve over time.

Q6a: On what grounds might Ofcom be prepared to grant a provider extra time to complete a risk assessment?

3.10 In general, we expect that in-scope services would be undertaking preparatory work ahead of the regime coming into force, so that they can move quickly once it's in place. As

mentioned above, we intend to form constructive relationships with in-scope services before the regime is in place, and as part of our engagement with them will seek to ensure they understand the requirements the Bill will be introducing. We think this will help providers prepare to bring themselves into compliance with the new regime on time so far as possible.

3.11 However, we acknowledge that there may be reasons why a provider might require additional time to complete a risk assessment. Any request for an extension of time would need to be considered on its merits, and it is therefore not possible to be exhaustive as to the reasons such an extension might be granted. But generally, we expect that we will be mindful of factors outside of a provider's reasonable control which mean that it would struggle to provide a complete and adequate risk assessment by a certain time.

4. Audit

Q8: How will Ofcom assess the safety and proportionality of i) automated moderation and ii) recommender tools?

Use of automated technologies to identify harmful content

4.1 Under the draft Bill, there are a few areas in which Ofcom might assess the use of automated moderation tools. Firstly, in line with their safety duties, platforms will have to be transparent in their terms of service about their use of automated technologies in relation to the identification or removal of harmful content. Separately, under the use of technology power, Ofcom can require the use of specific accredited automated technologies in certain limited circumstances.

4.2 In relation to platforms' proactive decisions to use automated technologies, there are a few different ways in which Ofcom will be able to set out its expectations of safe and proportionate use.

4.3 Ofcom will consider giving guidance in codes of practice about what information providers should give to their users about use of such technologies. In line with the duties under clauses 12 and 23 of the draft Bill, Ofcom could explain in codes of practice that we expect providers to take into account the importance of protecting users' rights to privacy and freedom of expression when deciding on what automated technologies to use, and how to implement them. Although we cannot say at this stage precisely what we might say in codes of practice in relation to this, we might, for example, recommend that providers should consider the effectiveness and accuracy of such tools in terms of how frequently they correctly identify the relevant type of illegal/harmful content compared to how often they wrongly identify such content, and that where there is reason to doubt that these tools are capable of identifying violating content to a reasonable degree of accuracy, decisions on removal of content should be referred to a human moderator for a decision. Providers will also have to put in place complaints handling processes which would enable

users to complain if they believe their content has been wrongly taken down or they have wrongly had their use of the service restricted, and for providers to take appropriate action as a result of such complaints (per the duties in clauses 15 and 24). Category 1 and 2 providers may also be required to report on their use of such technologies in their transparency reports.

4.4 In relation to the use of technology power and as mentioned above, under the draft Bill, Ofcom would only be able to *require* the use of *accredited* technologies, that meet *minimum standards of accuracy* decided by the Secretary of State, where the relevant conditions are met, and only in respect of CSEA and terrorism content (as discussed further below). Ofcom will carry out research with a view to providing advice to the Secretary of State about relevant minimum standards of accuracy for such technologies. We would also need to establish an accreditation process to identify and accredit technologies that would meet the relevant accuracy standards.

Recommender algorithms

4.5 We expect platforms to consider the impact recommender algorithms have in their risk assessments and, in accordance with the safety duties, to put in place appropriate mitigations for risks relating to recommender algorithms which they identify. Understanding the implications recommender algorithms have on online safety will be a key focus for Ofcom in the early years of the regime. We will use a combination of our own research and technical analysis and platforms' transparency reports (supported by our information gathering powers as needed) to better understand the impact recommender algorithms have on the propagation of harmful content online and on users' ability to make informed choices about what content they view, so as to help make informed decisions about how to target our regulatory activity in respect of these. Our work on this is already underway, including through the DRCF which identified algorithmic processing as one of the four priority areas for strategic work in 2021-22.

4.6 We expect platforms to consider the impact recommender algorithms have in their risk assessments and, in accordance with the safety duties, to put in place appropriate mitigations for risks relating to recommender algorithms which they identify. Understanding the implications recommender algorithms have on online safety will be a key focus for Ofcom in the early years of the regime. We will use a combination of our own research and technical analysis and platforms' transparency reports (supported by our information gathering powers as needed) to better understand the impact recommender algorithms have on the propagation of harmful content online and on users' ability to make informed choices about what content they view, so as to help make informed decisions about how to target our regulatory activity in respect of these. Our work on this is already underway, including through the DRCF which identified algorithmic processing as one of the four priority areas for strategic work in 2021-22.

Q9: The ICO has written to us about their audit powders. Could you set out to us where you think your powers under the draft Bill are comparable and where they differ? In particular, could you set out how the ICO's ex-post and ex-ante audit powers compare to the power to request a skilled person's report that you discussed with us?

4.7 We consider that Ofcom would have broadly similar investigative and information gathering powers under the draft Online Safety Bill to those ICO has to carry out audits. Under the Data Protection Act 2018, the ICO is able to:

- conduct audits with the data controller or processor's consent to identify areas of potential risk and assess whether they are complying with good practice (under section 129); and
- upon written notice, carry out assessments of whether a data controller or processor is complying with data protection law (under section 146). The ICO's powers when carrying out such an assessment include the power to enter specified premises, obtain or inspect information, documents and equipment, observe processing of personal data and interview company officers and staff. The ICO must normally give 7 days notice before providers have to comply with such a notice, unless there are reasonable grounds to suspect non-compliance with data protection law or an offence under data protection law and in the Commissioner's opinion compliance with the notice in less than 7 days is necessary (i.e. it is urgent).

4.8 The ICO has published guidance in which they explain their approach to audits under these powers. In this guidance, they state that they "predominantly conduct consensual audits under the provisions of s.129 of the Data Protection Act", and that an audit will "typically assess the organisation's procedures, systems, records and activities in order to:

- ensure that appropriate policies and procedures are in place;
- verify that those policies and procedures are being following;
- test the adequacy of controls in place;
- detect breaches or potential breaches of compliance; and
- recommend any required changes in control, policy and procedure".

4.9 Under the draft Online Safety Bill, Ofcom would have power to:

- require service providers, and other organisations, to provide us with information they hold or are able to generate or obtain for the purpose of exercising, or deciding whether to exercise, any of our online safety functions, including for the purpose of assessing compliance (clause 70);
- obtain a skilled persons report to: (i) identify and assess a failure or possible failure by a provider to comply with a relevant requirement; and/or (ii) to develop our understanding of the risk of a provider failing to comply with a relevant requirement, and how to mitigate that risk, where we reasonably believe the provider may be at risk of non-compliance (clause 74). Providers are required to give the relevant skilled person all such assistance as they may reasonably require to prepare their report;

- require certain individuals (including present or former employees) to attend interviews, as part of an investigation into potential non-compliance with relevant requirements (clause 76);
- enter and inspect premises, observe the carrying on of a regulated service by the provider, inspect documents and equipment found on the premises, and require the production of documents and explanations of documents (clause 77 and Schedule 5). These powers can be exercised without a warrant if we give at least 7 days' notice. Alternatively, they may be exercised without notice if we obtain a warrant, which we may do where the provider has unreasonably failed to comply with an earlier entry notice, or giving 7 days notice' would defeat the object of entry to the premises, or Ofcom require access to the premises urgently.

4.10 We consider that together these powers would enable us to assess providers' procedures, systems, records and activities in order to determine whether they are failing to comply with their duties under the Bill, and take enforcement action where required.

5. Accountability

How will Ofcom monitor, assess, and report on how they implement their duties in the Bill?

5.1 We would expect to monitor, assess and report regularly on how we are fulfilling our duties, including through Ofcom's Annual Report (which is required by paragraph 12 of the Schedule to the Office of Communications Act 2002) and in accordance with the duties that the draft Bill places on Ofcom to report publicly in relation to a number of our new online safety functions. For example, Ofcom will be making at least annual transparency reports (under clause 100), is required at least every three years to review and report on the severity and incidence of content which is harmful to children or adults (under clause 47), to report annually on the use of technology power (under clause 69), and to report within two years of commencement on researchers' access to information (under clause 101). We are also required to keep our industry-wide risk assessment (under clause 61) up to date, meaning we will be regularly reviewing it and seeing whether any changes may be needed.

5.2 The Government and Parliament each have important but distinct roles to play in maintaining oversight of Ofcom's activities and holding us accountable. We are keen to ensure that the regime is as open and transparent as possible, and that Ofcom can be held to account for the decisions we make, in particular given the novelty of the regime. As we have discussed, there are a number of mechanisms in the Bill for Government and Parliament to do this, and we believe it is for Government and Parliament to decide both as to the degree of discretion afforded to Ofcom, as well as whether the degree of oversight and input to our activities afforded under the draft Bill are right.

5.3 We understand that the Joint Committee is interested in exploring whether additional mechanisms of parliamentary oversight should be introduced, such as a standing Joint Committee. As mentioned in our oral evidence session and above, we recognise the

importance of Parliament having sufficient oversight of our activities – as a statutory regulator, we are ultimately accountable to Parliament and expect to be held to account for how we carry out the duties that Parliament has given us. At the same time however, it is important that Ofcom is able to carry out its activities in a robust and timely manner. If any additional mechanisms of oversight of Ofcom's activities were to be introduced, it would also be important to ensure that this is not duplicative of any of the existing oversight mechanisms already in place and that it would not inhibit Ofcom's ability to move at pace or to respond swiftly to emerging areas of concern.

6. Use of technology notices

Q11: Ofcom has raised concerns the threshold that CSEA content be "prevalent" or "persistently prevalent" on services before a use of technology notice can be issued is too high. What solution do you propose?

6.1 As explained in our technical note of 15 October, if we are given powers to require use of technology to identify seriously harmful content, we will need to be able to use them effectively. At present, the draft Bill requires us to demonstrate that there is evidence of persistent and prevalent CSEA and/or terrorism content on a service before Ofcom could require use of technologies to identify and remove such content. It is not currently clear how we would obtain evidence that this threshold would be met if services are not using technology to identify such content and its prevalence on the service, particularly in relation to private channels where there may otherwise be very limited visibility. In addition, it is unclear how thresholds might be set consistently across different services.

6.2 We recognise that given the use of such technology may interfere with users' rights to privacy and freedom of expression it is appropriate that a high threshold applies before such powers can be used. In line with the approach taken by the Courts when assessing whether such an interference with those fundamental rights is justifiable, we consider that requiring use of such technology should only be permitted where it is *necessary and proportionate to prevent the risk of harm* posed by such illegal content being present or disseminated via the service in question. In considering the circumstances in which use of such technology is necessary and proportionate, rather than evidence of persistent and prevalent CSEA/terrorism content being determinative of this question (as under the draft Bill currently), we think the Bill could instead enable us to assess a wider range of relevant factors. We are having constructive conversations with DCMS and the Home Office about how this can be achieved and have suggested that we think these factors could include the following:

- The nature of the service and its functionalities;
- The user base of the service;
- Any evidence Ofcom has as to the prevalence of relevant illegal content on, or disseminated by, the service (because particularly on a public channel an absence of such evidence may well indicate there is not a significant problem) and the relevant

time period this evidence covers (because the longer the time period, the more likely it is that there is an ongoing problem);
- The level of risk of, and severity of, harm to UK individuals if the relevant technology isn't used by the service;
- Any systems or processes already used by the service to identify and remove the relevant illegal content;
- The degree of interference posed by the use of the relevant technology with users' rights to freedom of expression and privacy; and
- The costs to the service of implementing the use of the relevant technology.

6.3 As also explained in our last letter, we also think it is important that the Bill is clear about the intended interaction between the use of technology power and the proactive steps to identify priority illegal content envisaged in the illegal content safety duties. In particular, we think it is important the Bill is clear whether there may be any circumstances where providers may be expected to use technology to identify and remove illegal or harmful content without being required to do so by Ofcom via a use of technology notice, and where failing to do so could mean that they are in breach of their duties. If Parliament envisages that there are circumstances where proactive use of technology may be a step required to comply with the illegal content safety duties, but outside of the specific use of technology power, options to provide such additional clarity could include:

- Setting this out expressly in the illegal content safety duties: for example, as part of a non-exhaustive list of steps which providers may, in some circumstances, be expected to adopt to comply with the duties, where it's proportionate in the circumstances;
- More tightly defining the scope of the use of technology power and what it applies to (e.g. amending clause 64(4), which sets out that the scope of this power applies to use of technology (i.e. any technology) to identify CSEA content and public terrorism content present on the service and swiftly take it down, including by means of the technology together with the use of human moderators – principles of statutory interpretation mean this is likely to preclude Ofcom having power to do something equivalent under any other provisions of the Bill).
- More tightly defining what actions Ofcom would be able to require providers to take to bring themselves into compliance with the safety duties as part of enforcement action (e.g. amending clause which presently prevents Ofcom from imposing any requirement to use technology to identify a particular type of content present on the service with a view to taking it down).

7. One-to-one services

Q12: Do you support the inclusion of private messaging services within the scope of the Bill?

7.1 We understand the rationale for including private messaging services (including online messaging services, video chat services and voice call services that involve more than one

person) in the scope of the Bill given they can be a vehicle for online harm, including some serious illegal harms.

7.2 For example, in online grooming where a perpetrator will seek to move a child from an open public forum to a private forum where the abuse occurs. Similarly, it is often the case that private channels are increasingly being used to disseminate terrorist content especially as a number of the violent extremist organisations have been proscribed by the Government or banned by social media companies. For example, research by the Institute of Strategic Dialogue in 2020 showed that 60% of private channels monitored (encompassing over 1million posts) had content supporting terrorists or terrorist organisations.

7.3 But we also acknowledge that regulation of the content transmitted via such services risks interfering with users' rights to privacy in relation to such communications, which needs to be taken into account when deciding what it is appropriate and proportionate for providers to do in protecting users' safety. We discuss these considerations further below.

Q13: Have you identified strategies to identify online harms in private messaging services which are end-to-end encrypted beyond i) user reports and ii) the use of meta data?

7.4 We acknowledge that there are particular challenges in identifying content on such services. We have been undertaking research to understand what techniques are presently available, or may be developed in future, to identify harmful content in relation to end-to-end encrypted services. The client-side solutions we are exploring include not just end-to-end encryption but also parental controls, media literacy and browsers.

7.5 There are a number of Privacy Enhancing Technologies (PETS) that are either being developed or being proposed that enable scanning to be performed in a privacy enhancing environment. We are maintaining a close interest in the development of these technologies, particularly as additional research begins into the appropriate governance structures once they are technically robust. We are also engaging actively with relevant stakeholders, including NCA, GCHQ, the Government and our DRCF partners, where we are undertaking a specific piece of joint work on end-to-end encryption.

Q14: How will you balance user privacy and the mitigation of potential harms communicated on end-to-end encrypted services?

7.6 All services, including services that permit private messaging or forms of private communication, will have to comply with their duties of care. This will include carrying out a risk assessment which will have to consider how the design and operation of the service may reduce or increase any identified risks – we consider this would include the fact a service is end-to-end encrypted. And all services will have to comply with their illegal content safety duties, and those that are likely to be accessed by children will also have to comply with the duties relating to content that is harmful to children. This will include taking proportionate steps to mitigate and manage the risks identified in their risk

assessments, to minimise the risk of dissemination of illegal content and to protect children from harmful content, although what will be proportionate in the circumstances will depend on the nature of the services, including use of end-to-end encryption, and the provider's size and resources (per clause 9(6) and 10(6)).

7.7 As set out above, when it comes to the regulation of online services that enable users to make private communications to one another, Ofcom recognises that it will be important to take users' rights to privacy into account when setting codes of practice that recommend steps providers may take to protect their users from harm, and when considering enforcement action against providers for failure to comply with the duties. In line with our own duties as a public authority under the Human Rights Act, we can only take action which would involve interference with users' privacy rights where the relevant action would be proportionate to the risk of harm that we are trying to prevent. This will be the case regardless of whether or not the platform is end-to-end encrypted, or encrypted or secured in some other way.

7.8 As noted above, however, there are particular challenges associated with end-to-end encrypted services, as their ability to identify harmful content being disseminated via such services is presently limited, and it is not yet clear to what extent these challenges could be overcome as a result of further technological developments.

7.9 We think it is a question for Government and Parliament as to where the line should be drawn between requiring providers of such services to take proactive steps to limit the dissemination of harmful and illegal content on such services, and preserving users' rights to privacy on such services. Given the absence of an express power in the draft Bill, we do not consider that there are any circumstances in which we could force providers to remove end-to-end encryption. Due to the security and privacy benefits associated with end-to-end encryption, and the public policy questions that may arise, we believe this approach is appropriate.

8. Age Appropriate Design Code

Q15: You told the Committee "we think that the Government's definitions here broadly, in fact more than broadly, capture all the services that children are spending their time on." Could you send us a comparison between the scope of the Age Appropriate Design Code and the draft Bill? Which services likely to impact on children do you believe are not covered by either the Code or the draft Bill?

Q16: Do you think there is a potential gap in respect of commercial services that do not have user-to-user content, but nonetheless fall under the Age Appropriate Design Code?

Q17: Do you think that regulatory alignment in this area would be useful and that the draft Bill might be extended to cover commercial providers than are regulated under the Age Appropriate Design Code but do not host user-to-user content?

Q18: Would such alignment close perceived loopholes, for example that commercial pornography services can avoid the provisions of the draft Bill by removing user-to-user functionality or that App Stores can include age inappropriate content?

8.1 As mentioned in our answers above, it is important that the online safety regime and data regimes are complementary and we will continue to work closely with the ICO across these issues.

8.2 As you are aware, the scope of the Age Appropriate Design Code (AADC) is different to the Online Safety Bill. The AADC is applicable to all 'information society services' (meaning any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services) that are likely to be accessed by children. The purpose of the code is to set out standards that online services 'likely to be accessed by children' must meet to ensure that they use children's data fairly and in compliance with data protection law. The ICO has set out that it expects online services to take a common sense approach to the question of whether their service is likely to be accessed by children. They are expected to take into account factors such as: whether the nature or content of the service has any particular appeal for children; the way in which the service is accessed, and any measures put in place to prevent children from gaining access. If the service is a kind that they don't want children to use in any case, online services are encouraged to focus on how to prevent access rather than to make it child-friendly. Examples given of these types of services include adult only and restricted services.

8.3 By contrast, the scope of the online safety regime focuses on online services which are search services or which facilitate the sharing of user-generated content (and regardless of

whether or not they are normally provided for remuneration). User-to-user services and search services that are not likely to be accessed by children will still be in scope and subject to the illegal content duties (and the duties related to content that's legal but harmful to adults if they are Category 1 services), although the specific duties relating to protecting children will only apply to those services which are likely to be accessed by children. In this context, 'likely to be accessed by children', as defined in the draft Bill, means that it is possible for children to access the service or any part of it (and a provider is only able to determine that it's not likely to be accessed by children if there are systems and processes in place that achieve the result that children are not normally able to access the service or that part of it); and the service (or relevant part of it) has a significant number or proportion of child users, based on evidence of who actually uses the service, or it is likely to attract a significant number of UK child users.

8.4 This means that all user-to-user services and search services which are actually likely to attract a significant number of child users – unless exempt – will be subject to the child protection duties in the draft Bill, even if they are intended to be 'adult only', unless they can ensure that in practice children aren't normally able to access them (e.g. they have robust age verification processes in place). This appears to be consistent with the approach under the AADC.

8.5 We are aware that there is parliamentary interest in whether there is a gap in relation to commercial porn services, where those services host content that is not user-generated. As mentioned in our oral evidence session, we recognise there is a risk that if they are not included in scope of the regime then the harmful content that can be hosted on these sites may move onto unregulated services. In terms of app stores, we recognise that they would not themselves be in scope of the draft Bill – although apps that offer search services or host user-generated content would be.

8.6 We understand the Government's decision to focus on user-to-user and search services for this regime, and our research suggests that these are the types of services which are most popular with users. For example, our latest Online Nation research found that just under half of 10 year olds use social media, rising to three-quarters of 12 year olds, and 88% of 8-15 year olds use search engines. Our research also found that more than half of 12 to 15 year-olds reported having a negative experience online in 2020.

8.7 The question of what types of services should be covered by the regime is ultimately one of policy, which will rightfully be decided by the Government and Parliament. But as we mentioned in our oral evidence session, there is a point at which a line has to be drawn around the scope of the regime so that we can ensure that the job we are given is a manageable one through which we can make meaningful improvements to users' online safety.

9. Age assurance and verification

Q19: Richard Wronka said: "We certainly see privacy-preserving and effective age verification measures as the kind of thing where we would look for extra specificity in the safety duties." What specific amendments are you looking for?

9.1 As explained in our previous letter, while we think it is right that the Bill provides for enough flexibility for services to take a different route to compliance where this is needed (for example, where developing new solutions or technologies) it is important that it also enables Ofcom to enforce effectively where platforms are not meeting the duties required by the legislation.

9.2 Platforms will be subject to duties to take steps to protect their users from illegal content and content that is harmful to children, and Ofcom will be able to set out recommend steps for complying with these duties in codes of practice. However, the codes of practice will not themselves be legally binding – and providers will be free to take alternative steps to comply with the safety duties. With the safety duties specified at a high level, it will therefore be harder for Ofcom to assess compliance, and to demonstrate non-compliance in situations where platforms take a different approach to the codes of practice.

9.3 At present, there is no express reference in the safety duties to the possibility that providers may be required to introduce age assurance systems to prevent or protect children from accessing harmful, age inappropriate content. While these measures may not be necessary for all in-scope services (for example, where the risks of harm to children from their services is limited), we think it would be helpful if the Bill were to include a non-exhaustive list of steps that providers may be required to take to fulfil the safety duties where proportionate, including reference to steps to control which users (including child users) are able to access the service (or relevant parts of a service) or to introduce systems for assuring the age of users. In addition to age assurance, other steps in the Bill that may be necessary for providers to take to comply with the safety duties might relate for example to user support measures (which could include offering parental controls).

9.4 Including additional detail in the Bill as set out above would make it clear that it may be necessary for providers to take such steps to comply with the safety duties where this is proportionate to the risk of harm, and it may therefore assist Ofcom in taking enforcement action if providers don't take these steps in circumstances where they would be recommended in the codes of practice and the provider's alternative steps are not effectively addressing those risks. A further option could be to consider amending clauses 9(6) and 10(6) of the draft Bill (which currently explain that 'proportionality' for the purposes of clauses 9 and 10 requires consideration of the findings of the risk assessment and the size and capacity of the provider), to also include reference to the extent to which the non-exhaustive list of steps, as described above, could effectively address the reasonably foreseeable risks of harm or whether they might be as effectively addressed in other ways.

Q20: As the draft Bill is currently constructed, would Ofcom be able to set binding minimum standards for privacy and effectiveness for companies who build their own age assurance systems? Would Ofcom be able to set binding limits on what a company commissioning a third-party age assurance service would be able to ask for from that service in terms of data?

Q21: It has been suggested that Ofcom do not have the technical capacity to set a code in respect of age assurance, so would recommend voluntary standards.

Do you believe Ofcom have the technical capacity to set a binding code of practice with minimum standards (both technical and governance) for age assurance?

If not, how could it effectively ensure that companies are complying with any voluntary code?

What would it do in respect of those companies that don't adopt the voluntary code?

9.5 Under the draft Bill, Ofcom will have the ability to set out recommended steps in codes of practice which would explain the circumstances in which providers may be expected to make use of age assurance measures, and the sorts of factors that we think providers should consider when deciding how to design an effective age assurance approach. As noted above, however, Ofcom's codes of practice are not legally binding, so providers could choose to adopt alternative approaches while still complying with their safety duties. Therefore, if providers adopt age assurance approaches which do not meet standards for age assurance that Ofcom has recommended in codes of practice, the failure to meet those recommended standards would not, in and of itself, mean they were in breach of the safety duties. As also explained above, Ofcom would welcome further specificity in the safety duties as to when age assurance should be adopted by providers to enable Ofcom to take action where providers are failing to use appropriate age assurance mechanisms. However, these proposed amendments would also not enable Ofcom to set binding standards for age assurance. It follows that Ofcom would have no power under the draft Bill to set any binding standards relating to age assurance. However Ofcom could enforce against providers where Ofcom could prove they weren't complying with the safety duties – for example, if Ofcom could show that the age assurance mechanisms that they were using were not effectively minimising the risk of children being exposed to harmful content on the service.

9.6 We also anticipate that most in scope providers will also have to comply with the AADC too, and to the extent they are failing to comply with the requirements of data protection law in their use of age assurance approaches, they may also face enforcement action by ICO.

9.7 We have already built significant technical and policy expertise around age assurance, for example through our work on VSPs, and relationships with providers of age assurance and

age verification systems. We are also working closely with Government on relevant safety by design and age assurance initiatives. Coupled with our existing standards expertise, we believe we are well placed to continue our preparations for our new online safety duties.

9.8 We intend to have a meaningful role in supporting standards for age assurance, and as part of our work to develop our codes of practice and on age assurance we are considering how best to support standards and certification schemes and the ways they can assist with compliance with regulatory obligations. In doing this, we will continue to ensure that we consider alignment with international standards where relevant.

10. Differences in legislation across the UK

10.1 Towards the end of our oral evidence session, a question was raised by John Nicolson MP about the differences in legislation across the nations in the UK, which we did not have time to answer fully. Ofcom recognises that there are differences in the criminal law across the UK nations and that as a result there could be divergences between the definitions of illegal offences under the different legal systems, such as the definition of hate crime and CSEA offences. We are considering the implications of this with Government and with input from our team in Scotland. Our teams continue to work closely with governments across the UK to understand what the different legal frameworks across the UK mean in practice for the implementation of the regime.