Your response

Introduction

This is a **joint submission** by Meta Platforms Inc. and WhatsApp LLC.

Meta Platforms Inc. together with WhatsApp LLC welcome the opportunity to participate in this inaugural consultation under the new Online Safety Act ("**OSA**") organised by the Office of Communications (Ofcom), calling for inputs on the development of guidance and Codes of Practice focusing on illegal content ("Protecting people from illegal harms online"). We also want to take this opportunity to thank Ofcom for the extensive research as well as the industry and expert outreach carried out over the last three years, which informed this consultation work.

We are committed to protecting our users' voices and helping them connect and share safely. In order to achieve this, we have invested significant resources - both human and technology. This is an ongoing effort and one that will continue to evolve over time. As such, we share the OSA's objectives to make the internet safer while protecting the social and economic benefits it brings to UK citizens.

Over the last several years, we have supported the development of the UK Online Safety framework by working with both the UK Government and Parliament. We are convinced that new and innovative regulatory frameworks must strike a complex balance between safety and people's rights, such as freedom of speech. Providers need to take their share of the responsibility to support how to strike this complex balance. We welcome Ofcom's approach throughout this consultation process to develop this regulatory framework by focusing on how to implement the safety duties efficiently, as well as the clear objective to develop guidance and Codes of Practice based on the principles of proportionality and collaboration.

At the outset, Meta Platforms Inc. ("**Meta**") reiterates and builds on two of the most important points from our previous contributions towards shaping an effective and workable online safety framework.

First, Ofcom's main priorities and objectives for the guidance and Codes of Practice should be **clarity**, **proportionality**, **flexibility**, and where possible **harmonisation with other content regulations**:

- The guidance and Codes of Practice are intended to expand on the broad duties set out in the OSA and provide the practical detail that providers need to comply with those duties. Regulatory certainty will be invaluable for providers, and therefore guidance and Codes of Practice should be as clear as possible in setting out how providers can comply with their obligations.

  Our detailed response indicates where we think the draft consultation materials would benefit from further clarity. However, we emphasise that Ofcom can be clear without being overly prescriptive or departing from the principle of proportionality that underpins the OSA's duties. While the draft consultation materials seek to differentiate between providers on the basis of size and risk, and offer a degree of flexibility in how providers can comply with their duties while remaining within the 'safe harbour' of the measures proposed in the Codes of Practice, there are a number of points where we consider the recommended measures to be overly prescriptive and / or disproportionate, or that the options are too

limited and not fully reflective of the current state of the industry as flagged in our response. This impacts the practicality of certain measures, and does not reflect that there are multiple effective ways for providers to meet the OSA's requirements and for which providers should benefit from a safe harbour.

- As Ofcom is aware, for the European Union, providers are also required to implement various measures in relation to illegal content, transparency and content moderation under the EU Digital Services Act (the "**DSA**") and some providers are subject to the additional requirements applicable to very large online platforms ("**VLOP**s") such as risk assessments. Meta appreciates that Ofcom is aware of the importance of harmonisation for systems at scale - however Meta has stressed further areas in the detailed response where this should be made more explicit. Greater flexibility for providers, as discussed above, would also make it easier for providers to harmonise their OSA-related measures with the measures required under the DSA and other legislation.

Second, the OSA grants Ofcom very broad information-gathering and enforcement powers, with significant penalties – including criminal liability – for non-compliance. Given this, it is **essential that there is a clear, measured and proportionate approach to information-gathering and enforcement**, which allows Ofcom to regulate effectively while avoiding intrusive and burdensome application of powers to providers who are seeking to engage productively with Ofcom. We welcome Ofcom's indication that it will seek to resolve issues constructively with service providers in the first instance, without pursuing formal enforcement action, and that it will take a proportionate approach to the use of its information-gathering powers. However, providers would benefit from further clarity on Ofcom's intended use of its powers, as discussed at various points in our detailed response. We have also identified certain aspects of Ofcom's proposed approach which, in our view, depart from established best practices under other regulatory regimes. As addressed in our detailed response, we consider that following such practices for the OSA would contribute to fairer and more effective regulatory outcomes.

Third, WhatsApp LLC ("**WhatsApp**") reiterates as well some overall concerns about specific elements of the regime. As Ofcom will be aware, in its end-to-end encrypted (E2EE) **private messaging** service, WhatsApp does not have access to the content of conversations on the service. In order to protect our users and society from harm on WhatsApp, while strongly protecting user privacy, we strive to design the environment to prevent users from encountering harm in the first place, and to empower people to keep themselves safe if they do encounter harm.

As we have detailed in previous calls for evidence and engagements with Ofcom, we have a comprehensive approach to addressing the risk of harm which may be encountered by users based on:

- Preventing abuse through product design, product functionality and features;
- Providing a strong suite of user controls which empower users to control their experience and keep themselves safe on the service;
- Designing ways to remove users who violate our policies or use our service to cause harm;
- Collaborating with external experts and organisations on safety measures and educational campaigns; and
- Working with law enforcement, in addition to responding to legal requests.

Meta and WhatsApp are convinced that constructive dialogue is essential to create a workable regulatory framework for all stakeholders while setting up evidence-based good practices and principles. Building on years of experience in tackling these issues through establishing policies,

building tools and technologies, in partnership with experts both within and outside our company, we welcome the possibility to share our expertise and learnings in this consultation response. To avoid duplication, we indicate for each question first the response by Meta and then, where applicable, the response by WhatsApp. The "us", "we", or "our" in the response refers to the respective entity named at the top of such response section. To avoid misunderstandings we sometimes refer to the "OSA" instead of "the Act" - both mean the same.

We appreciate the ongoing commitment of Ofcom to consulting with all the stakeholders in the development of the draft Codes of Practice, and remain ready to assist with further details on our answers.

******

Volume 2: The causes and impacts of online harm

Ofcom's Register of Risks

Question 1: **Response by Meta**
i) Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?
Response: We are grateful for Ofcom's extensive analysis and willingness to engage with providers of services on the cause and impacts of online harms and we acknowledge Ofcom's considerable effort to develop a register of risks based on three years of dedicated work. Meta has supported the UK Government's development of the Online Safety framework and shares the UK Government's stated policy objectives, to make the internet safer while protecting the vast social and economic benefits it brings to billions of people each day. We are committed to pursuing a constructive dialogue with Ofcom, and we welcome Ofcom's approach to establishing its consultation on in-depth research analysis. We also wish to highlight the value of online communication in general, and we share Ofcom's view, as stated in the consultation, that online services and functionalities are "*not inherently bad, and have important benefits*". We are deeply committed to offering our community the most positive, meaningful and safe experiences possible. To this end, Meta has developed the robust systems and processes it has in place to identify, manage, and mitigate risks on its services. A core part of our long-standing commitment to online safety and approach to risk management is a deep understanding of potentially problematic actors, behaviour and content that could arise via the design, use, or functioning of our services. Meta has had industry-leading content moderation processes in place for many years, which have evolved (and continue to evolve) to address changes in the online risk landscape. Leveraging this long-established integrity ecosystem, and in parallel to its DSA compliance obligations, Meta continues to build foundational integrity risk and compliance programme components that enable it to scale and build a risk and compliance programme fit for managing systemic risks into the future.

As part of our Integrity Risk Management Process, we identify, analyse, and assess the risks of harm that could stem from or be influenced by the following: problematic actors, behaviour, or content that violates our terms of service and/or may be considered illegal; application design or functionalities; or the use made of our services.

We provide the following comments on Ofcom's assessment of the causes and impacts of online harms in Volume 2:

Assessing Ofcom's evidence
Without having full access to all the evidence on which Ofcom's analysis relies, we are not in a position to fully engage with or assess that analysis or the conclusions reached by Ofcom.

Evidential gaps in Ofcom's assessment
We note that, as acknowledged by Ofcom in Volume 2 (e.g., at paras 5.14-5.17), Ofcom does not have the same quantity or quality of evidence for all areas of its assessment. We recognise that there will inevitably be gaps in the evidence available to Ofcom, given the wide range of services, risks and characteristics to be considered. In some cases, we expect providers may have unique information to hand, particularly as regards the way in which a specific risk manifests on the provider's service, which will factor into the provider's own risk assessment. We anticipate that Ofcom will take this into account where the conclusions reached by a provider's assessment depart from the broader conclusions set out in Ofcom's assessment.

Categorisation of online harms and how risk ratings should be derived for CSEA offences
Ofcom's explanations in the Consultation of the different kinds of online harms could, at times, be clearer as to how the 'CSEA offences' (Child Sexual Exploitation and Abuse offences) category of harm is treated, and as to how risk ratings for this category and its 'CSAM' (Child Sexual Abuse Material) sub-category are to be derived.

- Currently, Volume 2, Annex 5 (Draft service risk assessment guidance) and other consultation materials refer at various points to '15 kinds' of illegal harms because they group grooming and CSAM together as subsets of a single kind of illegal harm, referred to as 'CSEA offences'.

- However, Annex 5 (paras A5.40, A5.68-A5.69 and A5.74-A5.81) suggests that services should separately assess the risk of grooming, CSAM, image-based CSAM and CSAM URLs, and arrive at a separate high / medium / low risk rating for each of these – effectively treating each of these as distinct kinds of illegal harm for risk assessment purposes – as well as arriving at an overall risk rating for CSEA. It is not clear how this overall risk rating should be derived from the other risk ratings.

- These categories are again divided differently for the purpose of defining 'multi-risk' services; Annex 7 (Draft illegal content codes of practice for user-to-user-services, at p.48) defines a service as 'multi-risk' if it is assessed as being at least medium risk for at least two kinds of priority offences in accordance with the table at Annex 7 para A11.6. For the purposes of this definition, rows 2 (CSAM), 2A (image-based CSAM) and 2B (CSAM URLs) in that table are to be treated as one kind of priority offence, and row 3 (grooming) is to be treated as a separate kind of priority offence. However, if the provider has separate risk ratings for CSAM, image-based CSAM and CSAM URLs, it is unclear how these should be combined to derive a single risk rating for the first kind of priority offence, (particularly given that 'CSAM' covers other non-image-based and non-URL material, such as material

which contains advice about grooming or abusing a child sexually or which is an obscene article encouraging the commission of other CSEA offences).

We appreciate that different CSEA offences may present different risks and require different mitigations across services, as reflected in the CSEA-specific measures recommended in Annex 7. However, the consultation documents would benefit from clearer explanations of how the 'CSEA offences' category of harm is divided for different purposes and, in particular, how risk ratings for this category and the 'CSAM' sub-category are to be derived from the other sub-categories' risk ratings. We also note that NCMEC, the global clearinghouse for CSEA through its CyberTip reporting system has its own set of international standards which include the COPINE rating system, which categorises the severity of images of child abuse. It would be beneficial for the OSA to have aligned categorisation with these international standards.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: Please see our response to Question 1 (i) above.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 2: **Response by Meta**
i) Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.
Response: Please see our response to Question 1 above.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Volume 3: How should services assess the risk of online harms?

Governance and accountability

Question 3: **Response by Meta**
i) Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
Response: Our comments on the proposed governance and accountability measures are as follows. Each

measure is taken in turn.

All services:

Name a person accountable to the service's most senior governance body for compliance with illegal content duties and reporting and complaints duties.

Meta broadly supports this proposal and recognises the importance of building a culture that prioritises safety (as noted in para 8.48 of Volume 3) and of the importance of having engaged senior management oversight of risk.

In anticipation of the developing regulatory regime around online content, Meta has established a three lines of defence model of risk management, which includes a new Integrity Governance, Risk & Compliance Function ("**IGRC**") as part of its second line of defence. IGRC works to identify, manage and mitigate risks across Meta's products, remediate issues and facilitate effective reporting. Meta has established an IGRC Programme to provide ongoing risk governance and oversight of Meta's services, systems, and processes. This programme includes an Integrity Risk Management Process that pulls from "ISO 31000: Risk Management" as a leading practice, is tailored to meet the needs of our environment, and builds on the existing integrity measures we've had in place for years.

Meta is in the process of developing a dedicated UK Online Safety Act compliance team, who will work with IGRC's support to monitor Meta's compliance with the OSA and related CoPs, and facilitate reporting to senior management. Meta has also already provided Ofcom with the name of a senior leader in our Compliance Organisation (where the IGRC team sit) for the purpose of identifying a person accountable on an interim basis for Meta's response to online safety regulation and to whom Ofcom's initial supervisory letter dated 8 December 2023 could be addressed. As noted in our response to this letter, Meta is still in the process of standing up our compliance governance structures internally.

All multi-risk and all large services:

Senior managers named and statements of responsibilities created

Meta is supportive of the proposal to require written statements of responsibilities for certain senior members of staff. However, as a large, multi-faceted international organisation and in recognition of the multidisciplinary nature of online harms, the final proposal should maintain sufficient flexibility to adapt to the reality of a variety of organisational designs that may change over time. Organisational structures do not always remain static and responsibility may be shared across multiple individuals and teams. We would therefore wish for the proposal to remain sufficiently flexible to allow for this and guard against it becoming more prescriptive.

Further, given the sensitive nature of many online risks which we manage, we would be keen for Ofcom to be very clear on retaining the confidentiality of the statements of responsibilities and of the related names.

It should also be noted that the implementation and maintenance of such statements at a global, matrixed company such as Meta will likely require significant additional investment in human resource structures and processes. The estimate of an average time investment to create a statement of 'a few days' (para A8.74) is in our view too short.

Track evidence of new illegal harms

We explained aspects of our approach to identifying emerging risks in our response to the 2022 Illegal Harms Call for Evidence (as referenced in Volume 3, para 8.117) , and our risk intelligence team continues with its work on reviewing escalations across internal teams. We intend to continue to leverage our internal processes to meet this requirement. As stated above in response to Question 3, IGRC will also be involved in identifying risks that may emerge and ensuring these are reported internally.

Code of conduct

A Code of Conduct has the benefit of providing clarity to relevant Meta staff of their duties and obligations under UK law, and this is to be welcomed.

We would advocate for discretion on how to draw up the Code to maintain flexibility and ensure we can align its contents with existing internal and external Codes of Conduct with which Meta complies.

Training

Meta recognises that effective training is an important part of a compliance framework and already delivers extensive staff training across our business. We support the proposal that relevant staff involved in the design and operational management of the service receive training on the service's approach to compliance with the illegal content safety duties and the reporting and complaints duties, but, as with the Code of Conduct, would advocate for discretion and flexibility on the form and manner in which this training is delivered.

Annual Review of risk management activities

This proposal is complementary to Meta's commitments under the EU's DSA and is supported. Meta supports and encourages Ofcom's aims at harmonisation with other regulatory regimes around online harms. However, we would like the opportunity to comment on this further should Ofcom put forward its own review template. We would advocate for a proposal that is flexible and affords providers with sufficient discretion as to the design and operation of such a review.

Large multi-risk services:

Have an internal monitoring and assurance function to provide independent assurance that measures taken to mitigate and manage the risk of harm to individuals identified in the risk assessment are effective on an on-going basis, reporting to an overall governance body or audit committee.

We support this proposal. See our detailed comments earlier in this response on how, in anticipation of developing global regulatory regimes around online content, a three lines of defence model of risk management has been established at Meta, including a new Integrity Governance, Risk & Compliance Function (IGRC). As part of our three lines of defence model, we also have an internal audit function which provides comprehensive and independent assurance on the effectiveness of governance, risk management, and internal control activities.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: Please see our response to Question 3 (i) above.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 4: **Response by Meta**
i) Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response: We broadly support these proposals. However, please also see below our response to Question 12, in which we explain our concerns regarding the lack of clarity with regards to what constitutes a "service" and where the boundaries of a service should lie. In our view, it is not entirely clear from the OSA and the consultation documents where the boundaries of a service are drawn.
ii) Please explain your answer.
Response: Please see our response to Question 4 (i) above.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 5: **Response by Meta**
(i) Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?
Response: Meta does not support this proposal for a potential future measure for the following reasons. This does not appear to be a proportionate requirement. The OSA already provides adequate levers in the regulatory toolkit to enable Ofcom to get the information it requires to further its objectives in ensuring online safety for UK users, namely: ● the ability to issue an audit notice (OSA Sch 12 para. 4) and related powers in that paragraph; ● the ability to instruct a skilled person to produce a report; ● other information gathering powers, which may in practice be used to obtain information pertaining to Meta's compliance with its risk assessment and safety duties.

In many cases, providers of regulated services will have existing internal processes which would negate the need for an additional independent audit requirement, as follows:

- Meta already carries out effective internal audits;
- Meta has established an Integrity Governance, Risk and Compliance function that will perform a continuous cycle of monitoring, testing and improvement work, producing relevant materials that can be provided, as appropriate, to Ofcom during the supervisory relationship.

Lastly, the EU's DSA already requires Meta to conduct an annual independent audit and to produce an audit implementation report. This report will be made public and will therefore be available to Ofcom. This will provide annual and frank access to our integrity approach for the systemic risks as defined by the DSA. We recognise that the DSA's systemic risk matrix differs to that of the OSA, but we note that the DSA audit will examine integrity and safety matters that have some alignment with user safety matters that are relevant to UK users and that would be relevant to any potential OSA audit, including content reporting, complaints handling, risk assessments and risk mitigation measures (including in relation to illegal content and protections for children), and the provider's compliance function and risk management framework.

The DSA audit report will therefore provide a quantity of detailed and relevant information (in addition to any information that Ofcom may obtain via the information-gathering powers discussed above), rendering the costs and resourcing requirements of any further OSA-specific audit disproportionate. Ofcom has been clear that the UK Online Safety framework should complement and draw from the global system that is under establishment, and therefore building on the information provided through the EU framework rather than duplicating it represents an opportunity for Ofcom to make this a reality.

Importantly, a potential cost to Meta of such a measure is the opportunity cost associated with removing trust and safety experts from front line risk mitigation work, to manage and respond to an independent auditor. We are seeing from the DSA independent audit process that is currently underway that the work involved is very significant. Meta regards it as more important to have trust and safety front line staff, and risk and compliance second line of defence staff, focused on creative identification, management and mitigation of risks rather than being taken from this work to focus on audit requirements, especially in circumstances when other powers in the regulatory toolkit mean that Ofcom can gain visibility of areas of interest.

In conclusion, Meta's view is that the introduction of a further independent audit requirement does not add substantially to Ofcom's existing powers and the information it can receive from Meta through the supervisory relationship and access to the publicly available DSA audit report. As such, our view is that the costs of this measure would outweigh the benefits, and that it would be at odds with the principle of proportionality that underpins the OSA's requirements for providers.

Meta would be open to discussions with Ofcom about the cost of the DSA independent audit process to better highlight that an additional independent audit would be disproportionate.

(ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Question 6:

Response by Meta

(i) Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?

Response:

We do not support this proposal.

We recognise that remuneration and incentives are powerful drivers of compliant behaviour, but financial remuneration is not tied to performance in the tech sector in the same way as it is in financial services, for example. Establishing a causal link between a single decision and a suboptimal outcome will be very difficult at Meta, given our scale and complexity. The nature of online safety risks and the process of their management is wholly different, more nuanced and more complex as compared to risks seen in the financial services sector.

For example, the business model and employee incentive structure of a financial services firm may focus on sales to customers, with risks of harm to customers arising where employees are incentivised to sell products inappropriately or bypass compliance requirements to increase sales – i.e., with harm arising directly from wrongdoing by the firm's employees that is intended to increase firm revenues and their own remuneration. In this situation, directly linking employee remuneration to compliance KPIs can help to counteract the incentive for an employee to increase remuneration via wrongdoing.

In contrast, for a user-to-user service with a business model focused on, e.g., generating revenue from advertisers or from users themselves, the risks of harm to users will overwhelmingly, if not exclusively, arise from illegal or harmful content generated by other users (not from wrongdoing by the provider's employees). The prevalence of such content on the service is also liable to drive away users and advertisers, damaging the service's revenues and so potentially negatively impacting employee remuneration. As such, the provider's employees already lack a direct financial incentive to engage in wrongdoing, and are already incentivised to mitigate the risks of harm to users, making it unnecessary and superfluous to further tie remuneration to compliance measures.

Moreover, the suggested approach does not accord with the principles of intermediary liability that have been in place since at least 2002, when the e-Commerce Directive was implemented into UK law by the Electronic Commerce (EC Directive) Regulations 2002, and which remain in force following Brexit.

The preponderance of illegal harms is determined in significant part by external events, over which senior managers and intermediary service providers have no control. Meta monitors these events and has systems in place to respond accordingly. Meta is continually working to update its controls in response to the evolving threat landscape, including in monitoring evolutionary behaviours by bad actors regarding the misuse of our services. While our risk management practices are intended to identify and mitigate such risks on an ongoing basis, it is not always possible to prevent such misuse in real time, and as such, tying remuneration to online safety outcomes that may be determined in significant part by external events is not reasonable or proportionate. In short, whereas in the financial sector failures (and therefore remuneration) are linked to negative impacts directly caused by employees, in tech the harms are caused by users

and not employees. This degree of separation from the employee to the cause of the harm makes linking remuneration in the way suggested unfair, disproportionate and illogical.
(ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Service's risk assessment

Question 7: **Response by Meta**
i) Do you agree with our proposals?
Response: Our comments to the proposals are as follows. *Written policy in place for providers to review their risk assessments at least every 12 months, and to name a responsible person for overseeing this process* We support this proposal. *Services update their risk assessment whenever a 'significant change' to their service occurs* Art. 34 of the EU DSA requires a risk assessment to be carried out before deploying functionalities that could have a "critical impact" on the "systemic risks" identified in, and pursuant to, Art. 34 of the DSA. While recognising that the text of the OSA is fixed by Parliament, we wish to encourage Ofcom to pursue more harmonisation with the DSA in terms of interpreting the text of the Act to clarify what might constitute a "significant change" under the OSA. We could support the proposal if the definition of "significant change" were to align more closely with that of "critical impact" under Art. 34 DSA. However, Ofcom's guidance on what constitutes a "significant" change is novel and overly broad. The DSA allows providers to assess this on their own. Ofcom has proposed a number of bases on which a new assessment would be needed, including introducing a new recommender system or machine learning model, changing "content rules" (such as a Community Standard), changing the design of a reporting button or other icons for how users react to content, and even a change in headcount that "may affect the number and quality of technical resources to assess and mitigate risk of illegal harm" (Annex 5, para A5.135). This guidance is overly prescriptive, making it difficult to effect in practice. It being so prescriptive also renders it susceptible to becoming quickly out of date as online safety risks (and our internal systems to tackle those risks) continually evolve. In any one of the examples provided by Ofcom, there can be a large spectrum of changes that could occur, most of which should not meet this threshold and that needs to be made clear. For example, with regards to changes in headcount, IGRC would not necessarily be aware of the potential impacts which that change may have (or any downstream effects on risk) prior to that change taking place. In addition, stating that headcount changes are likely to be significant where they "may affect" the number and quality of technical resources does not reflect the fact that any potential effects may be unlikely, minor and / or compensated for through other means (such as

improvements in automation and other internal systems supporting productivity).

We also note that a number of the other examples of significant changes set out in the guidance are also based on the change having an 'impact' or 'effect', without specifying how material that impact / effect needs to be for the change to qualify as significant. For example, Annex 5 Table 13 states that a proposed change is "very likely" to amount to a significant change if it "impacts a vulnerable user group, such as children" or if it "impacts the efficacy" of measures put in place following the previous risk assessment to combat illegal content, without indicating how significant that impact should be, or what proportion of the vulnerable user group or anti-illegal content measures need to be affected. It is therefore unclear where the threshold lies for a change to be 'significant' in these examples.

While Ofcom may wish to provide some examples of the types of issues that may be in scope, such a list should be for illustrative or guidance purposes only and careful thought needs to be put into when such a change would meet the threshold of 'significant' which would ideally align with the standards found in Art. 34, DSA in order to reduce a potentially disproportionate burden.

ii) Please provide the underlying arguments and evidence that support your views.

Response: Please see our response to Question 7 (i).

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Question 9:

Response by Meta:

i) Are the Risk Profiles sufficiently clear?

Response:

We support Ofcom's aim behind the Risk Profiles to "give services a consistent starting point to understand risk on their services, based on Ofcom's sector-wide assessment on how harms manifest online (our Register of Risks)." (Volume 3, para. 9.54).

The tables of 'Risk Profiles' at Annex 5 Appendix A are helpful. Meta will consult these tables when doing our risk assessment and take the relevant risk factors into account. We note that the information in the Risk Profiles is a high-level summary of the most important risk factors, and is based on the Register of Risks, which sets out Ofcom's detailed analysis and evidence in full (including some risk factors that are not reflected in the Risk Profiles, due to having more limited evidence) (Annex 5 paras A5.136-A5.145).

However it should be recognised that Meta has many years of experience of identifying, managing and mitigating the risks posed by its services and will continue to use its own risk signals and analysis in addition to the Risk Profiles.

We therefore note and agree with Ofcom's comment that the Risk Profiles are a 'starting point' (A5.141).

ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 9 (i).
iii) Do you think the information provided on risk factors will help you understand the risks on your service?
Response: Please see our response to Question 9 (i).
iv) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 9 (i).
v) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Record keeping and review guidance

Question 10: **Response by Meta**
i) Do you have any comments on our draft record keeping and review guidance?
Response: Our comments on the proposals are as follows. *• Written records can be made and kept in a durable medium of the service's choice.* *• Where reasonably practicable, written records should be kept in English (or for services based in Wales, in English or Welsh.* *• Written records are written in as simple and clear language as possible.* We have no comment on these proposals. • *A written record must be kept of current risk assessments and compliance measures and must be updated whenever a significant change is made.* We broadly support the risk assessment record keeping proposals but are keen to understand related confidentiality provisions. Some of the information contained in risk assessments is likely to be confidential from both a commercial and from a safety perspective. • *Ofcom's expectation is that services should undertake a compliance review at least* ***once a year****, but more frequent reviews may be appropriate if the regulated service becomes aware of compliance concerns or implements new measures. Services should also carry out a* ***compliance review if there is a significant change*** *to any aspect of the design or operation of the service.* This proposal coheres with systems and processes Meta has put in place in order to comply, at scale, with a variety of global content regulations. and our plan would be to leverage our new internal compliance teams to effect this review. We welcome the ability to exercise discretion in how best to conduct such reviews over our various services, to ensure these reviews are bespoke and therefore optimal in achieving Meta's compliance aims, in alignment with our statutory

obligations.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 10 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 11: **Response by Meta**
i) Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response: We have no comment on this.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We have no comment on this.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Volume 4: What should services do to mitigate the risk of online harms

Our approach to the Illegal content Codes of Practice

Question 12: **Response by Meta**
i) Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
Response: Based on the services we provide, our response is focused on Annex 7 (Draft illegal content codes of practice for user-to-user services). We are grateful for Ofcom's clarity and candour in their process of development of the Codes of Practice ("**CoPs**") and we welcome this consultation process as it helps to ensure that impacts of options expressed in the consultation can be properly considered before CoPs are finalised. Based on the development of codes of practice we have seen around the globe, we believe that such instruments allow for greater flexibility to develop, adapt and respond quickly to ever-evolving technological environments. To that end we also appreciate that Ofcom is seeking

input from consultees on some topics that may only be addressed in future iterations of the CoPs, and that the CoPs will generally evolve over time as Ofcom learns more and the sector develops. Indeed, Meta's own experience in addressing different types of content and integrity issues, is one of ongoing development. Therefore, flexibility remains key.

We strongly support:

- Ofcom's aim to capture existing good practice within industry, set clear expectations, and work to raise standards of user protection over time, especially for services whose existing systems are nascent or under-developed. Platform integrity is as important as it is challenging in practice. We constantly invest in existing and new technologies/tools and processes to reinforce the integrity of our services and with years of expertise in this domain, we want to share our experience and learnings to level the playing field in this domain.
- Ofcom's acknowledgement of the advantages and aim of alignment with other content regulations, such as the DSA. This aligns the UK with global industry standards and best practices framework, e.g. similar efforts in the EU and Australia.
- Ofcom's commitment that the CoPs have to be based on proportionality and that expectations for services need to be clear.

As part of this response, in addition to feedback on specific measures, we would like to share **some preliminary suggestions and concerns**:

1. We noticed some potentially problematic **divergences from other regulations**.

In our view, it is essential to develop regulatory models which are workable within the full spectrum of other, relevant regulations for online services (such as privacy regulation) and the global regulatory environment, in order to avoid fragmentation of the technological landscape. As such, CoPs should avoid setting up dual regulatory regimes. We set out more details on this in our responses to Questions 13 to 47 below.

2. We believe that the **following proposals would help to support proportionality** in relation to the consultation and the regulatory model that will ultimately be adopted:

a) Clarity on boundaries of a service - and in case such guidance is not forthcoming, will be developed at a future date or those boundaries are drawn broadly - flexibility should be built in as to what proposed measures are required for different *parts* of such services that have different risk classifications

In our view, it is not clear from the Act or the consultation where the boundaries of a service are intended to lie. As an example, it is not clear whether Facebook (as accessed via, e.g., the Facebook App) is intended to constitute a single service or whether, e.g., "Facebook Dating" and "Facebook Marketplace" - which are accessible within the Facebook App but provide different service offerings and have different risk profiles - would amount to distinct, individual services.

The broader and narrower interpretations set out above each have comparative benefits. A narrow interpretation that means a provider's offerings are split into a large number of services may lead to a disproportionate number of work products (such as, e.g., transparency reports), which would be burdensome for providers and may also increase the regulatory burden on Ofcom. On the other hand, an

overly broad interpretation that groups multiple products with different risk profiles into a single service may mean that the entire service (including parts which have fewer users or a lower or more limited risk profile) is required to meet more onerous requirements that are applicable to large and / or multi-risk services, which may result in disproportionality.

We propose that Ofcom provides clarity on how the boundaries of a service will be drawn and, where that results in multiple products/parts of the service with different risk profiles being grouped into a single service, allowing the different parts of the service to be subject to proposed measures in line with their own size / risk level.

b) More options to constitute a 'safe harbour'

Compliance with measures recommended in the CoPs will effectively give providers a 'safe harbour' regarding their compliance with the Act. However, most providers will already have a range of safety and integrity measures in place, which will vary depending on the design and underlying integrity systems of the service.

Against that backdrop, we propose that Ofcom, rather than providing a single set of recommended measures that will constitute a safe harbour, suggests or allows for a range of options which would meet the objectives of the Act, to reflect the flexibility and variation among services.

We are aware that the Act permits providers to deviate from Ofcom's recommended measures, but providers that do so lose their 'safe harbour' and bear responsibility for proving their alternative measures are equally effective. If Ofcom were to provide greater flexibility in its recommended measures, this would make it easier for providers to build on their existing online safety measures, rather than feeling that they need to spend resources on replacing an established and effective safety framework with the CoP-recommended version in order to benefit from the safe harbour. It would encourage an ongoing flexibility of approach to user safety, which is essential in an environment of constant technical evolution.

c) Clarity as to how the 'safe harbours' available under the CoPs will apply to the relevant duties of the OSA

We note that s.49 OSA gives providers 'safe harbours', in that it states that providers will be treated as complying with a relevant duty if they take the measures recommended in a CoP for the purpose of compliance with that duty. We also note the index of recommended measures at pp.6-10 of Annex 7, which includes a column indicating which duty or duties a particular measure relates to. While this is a helpful reference, there are aspects of the index that we think could be clarified.

First, a number of measures state that the 'relevant duties' include those set out in various subsections of s.10(4). However, our understanding is that s.10(4) does not impose additional duties, but merely contextualises the duties in ss.10(2)-(3) by setting out areas of a service in which a provider may need to take measures to

comply with the ss.10(2)-(3) duties. It is therefore not clear to us why the index refers to the subsections of s.10(4) as if they were distinct standalone duties. For example, we note that the 'relevant duties' set out in the index for recommended measure 6A (regarding terms of service) include s.10(4)(c) – which states that the ss.10(2)-(3) duties may require measures to be taken in relation to policies on terms of use – but the relevant duties for this measure do not include s.10(2) or s.10(3). If a provider did not follow measure 6A and instead took an alternative measure, it is therefore unclear whether this would lead to the provider losing the safe harbour for the s.10(2) and / or s.10(3) duty.

Second, a number of measures state that the 'relevant duties' include an entire section, where that section contains multiple distinct duties – for example, measures 3A to 3D and 3F to 3G refer to s.10, which contains seven separate duties in subsections (2)-(3) and (5)-(9). It is unclear whether these references are intended to cover every duty in the section referred to – such that, for example, if a provider takes an alternative measure for measure 3B, the provider will then lose the 'safe harbour' for every duty in s.10. In our view, this would be disproportionate, particularly in situations where the provider's alternative measure may in practice consist of a slightly adjusted version of the recommended measure that, e.g., better fits its existing operations or the structure of its service. If this is not what is intended by the references to entire multi-duty sections, we suggest that the index is adjusted to clarify which specific duties are relevant by reference to particular subsections.

3. Timeline

Since the implementation of some measures proposed in the CoPs will depend on the results of the risk assessment, clarity in which month the final guidance for risk assessment is expected would be helpful for resource planning on such implementation work. Currently available timelines (as set out in, e.g., Ofcom's roadmap for implementing the Act) indicate such only by reference to a quarter.

4. End to end encryption ("E2EE")

Proposed measures and protections in case of E2EE remain a concern, please refer especially to the responses to Questions 1, 12, 16, 18 and 20.

5. Length of consultation

Finally, we would like to note that the consultation is extremely detailed, with the relevant documents totaling more than 1,700 pages. We suggest that for future consultations (e.g., regarding the Act's child-related duties), it may be more proportionate to separate topics into sub-categories and address them in separate (and shorter) consultations, to promote engagement with as many providers and stakeholders as possible.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Question 13:

Response by Meta

i) Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?

Response:

The draft CoPs set out a 'differentiated' approach to apply the most onerous measures in the proposed CoPs only to services which are large and/or medium or high risk. We understand this is intended to meet the principle of proportionality.

It is right that regulation takes account of the varying risks and capabilities of different services. Developing proportionate integrity solutions is not a static exercise, and there might be several ways to tackle issues and risks on platforms.

1. However, the draft CoPs make a flawed assumption by focusing at times only on size as a proxy for harm.

The Act tasks Ofcom when determining the proportionality of various safety steps to focus on the factors 'size and capacity' of the service "and" the service's own risk assessment (s. 10(10) OSA). While some of the measures in the draft CoPs apply at a proposed threshold of both risk level and size, others apply only at a proposed threshold of size and for others risk still remains a determining factor. The draft CoPs equate high reach with high risk, implying that services with the largest user base are higher-risk or that measures will have greater impact by means of higher reach.

Using size as a proxy for harm is a simplistic assumption as harm varies between services and is not necessarily related to the size of the service. Frequently, potentially hateful or dangerous narratives that emerge on our platforms were first developed and spread on smaller services or those with less sophisticated integrity measures. In addition, larger services are also subject to more frequent and in-depth scrutiny by their users, the media, regulators and other stakeholders. This scrutiny, and the associated reputational exposure, gives larger services a further incentive to be at the forefront of tackling online safety risks, in addition to the core goals of protecting user safety and the integrity of their services. We also note the tacit responsibility of more mature companies to support the development of the whole ecosystem - e.g., by participating in industry forums, sharing best practices and risk mitigation tools, and taking other such steps to help less mature companies to improve their internal systems.

Ofcom should consider a more equitable, risk-based approach that addresses risks where they appear.

2. We also refer to our concern regarding the lack of clarity as to where the boundaries of a service are drawn, as expressed in our response to Question 12 above. If the boundaries of a service are to be drawn broadly, Ofcom's recommended measures should allow for flexibility as to the measures that should be implemented on different parts of a service which have different risk classifications.

3. We note that the same concerns will also apply when considering how to define and draw the boundaries of Category 1 services, which we understand will be addressed in another consultation

phase.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 13 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 14: **Response by Meta**
i) Do you agree with our definition of large services?
Response: Please see our response to Question 13 on how, in our view, equating high reach with high risk is flawed. However, if a threshold is to be set for 'large' services: ● We agree that it should be aligned with thresholds in other content regulations, such as the DSA, i.e. average monthly active users equating to approximately 10 percent of the relevant population. ● Thresholds and methodology for calculations should be clearly defined. We refer to our concern set out in our response to Question 12 on the lack of clarity on where the boundaries of a service are to be drawn.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 14 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 15: **Response by Meta**
i) Do you agree with our definition of multi-risk services?
Response: We understand Ofcom defines a "multi-risk" service as a service which is high or medium risk for at least two kinds of illegal harm, based on the provider's most recent risk assessment. Based on this definition, it follows that a service which is high or medium risk for two kinds of illegal harm will be subject to the same stringent measures as a service that is high or medium risk for all 15 kinds of illegal harm. While we appreciate that it is difficult to define where to draw the line for 'enhanced' measures further proportionality could be considered.

As a matter of principle, we believe that risk assessment obligations should include overall guidance on the structure and content of the risk assessments, while ensuring sufficient flexibility for different services and adaptability for the future.

Further, the risk parameters in the table in the CoP in Annex 7 (p.64) need to be aligned with the parameters in the risk assessment guidance (Annex 5), as the determination of whether a service is "multi-risk" depends on the risk ratings derived during the course of the risk assessment. It should be clear to a service what tier of risk they fall into. See our response to Question 1 above in which we discuss the lack of clarity with regards to how certain risk ratings should be derived.

ii) Please provide the underlying arguments and evidence that support your views.

Response: Please see our response to Question 15 (i).

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Question 16:

Response by Meta

i) Do you have any comments on the draft Codes of Practice themselves?

Response:

Based on the services we provide, our response is focused on the draft CoPs for user-to-user-services in Annex 7.

We refer to our answers in Questions 12 to 15 on the general approach to classification of services which determines which measures are proposed by Ofcom for which type of service. As outlined, our response emphasises:

- greater alignment with other regulations and avoidance of dual regimes, and
- proportionality for measures, especially
  a) Clarity on boundaries of a service - and in case that is not possible or those boundaries are drawn broadly - flexibility as to what the proposed measures require for different parts of such services that have different risk classifications
  b) More options to constitute a safe harbour and
  c) Clarity as to how the 'safe harbours' available under the CoPs will apply to the relevant duties of the OSA.

In addition, we share the below specific remark on private messaging: We welcome Ofcom's clarification that the automated content moderation proposals it brought forward in the consultation are limited to content communicated publicly, where it is technically feasible to implement them, and that they will not apply to private communications or end-to-end encrypted communications ('e2ee'). We consider this appropriate given the potential for some of these proposals to compromise users' ability to trust in the privacy and security of their private messages - as well as the regulatory landscape applying to private messaging services which we expand upon in our answer to Question 21.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Question 17: **Response by Meta**
i) Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
Response: We appreciate the difficulties in estimating costs. As a general remark, we note such may vary from service to service, e.g. may be higher than set out in Annex 14.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Content moderation (User to User)

Question 18: **Response by Meta**
i) Do you agree with our proposals?
Response: We understand this Question refers to the proposed measures 4A to 4F in Annex 7. Please see below our feedback for these proposed measures. *<u>1. All services: Having a content moderation function that allows for the swift take down of illegal content (ref 4A)</u>* Ofcom recommends that the "*provider should have systems or processes designed to swiftly take down illegal content of which it is aware (a 'content moderation function'). For this purpose, when the provider has reason to suspect that content may be illegal content, the provider should either:* *a) make an illegal content judgement in relation to the content and, if it determines that the content is illegal content, swiftly take the content down; or* *b) where the provider is satisfied that its terms of service prohibit the types of illegal content which it has reason to suspect exist, consider whether the content is in breach of those terms of service and, if it is, swiftly take the content down."* Meta appreciates Ofcom offering two options as a proposed measure. We refer to our answer to the related Question 49 below for details. *<u>2. All 'multi-risk' or large U2U services: Setting internal content policies (ref 4B)</u>* Ofcom recommends that

- *"the provider should set and record (but need not necessarily publish) internal content policies setting out rules, standards and guidelines around: a) what content is allowed on the service and what is not; and b) how policies should be operationalised and enforced.*
- *The policies should be drafted in such a way that illegal content (where it is identifiable as such) is not permitted. In setting such policies, the provider should have regard to: a) the risk assessment of the service; and b) information pertaining to the tracking of signals of emerging illegal harm."*

We support Ofcom's recommendation that the provider should set and record internal content policies setting out rules, standards and guidelines on what content is permitted on the service and what is not; and how policies should be operationalised and enforced.

As regards the policy approach to illegal content, please see our comments on this point in our response to Question 49 below.

3. All 'multi-risk' or large U2U services: Performance targets (ref 4C)

This measure suggests that *"the provider should set and record performance targets for its content moderation function, covering at least:*
a) the time that illegal content remains on the service before it is taken down; and
b) the accuracy of decision making.
In setting its targets, the provider should balance the desirability of taking illegal content down swiftly against the desirability of making accurate moderation decisions. The provider should effectively measure and monitor its performance against its performance targets."

a) The OSA does not prescribe specific turnaround times for the removal of illegal content and instead provides a duty to operate a service using proportionate systems and processes designed to (a) "minimise" the length of time for which any priority illegal content is present; and (b) where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, "swiftly" take down such content.

While we appreciate Ofcom's approach not to prescribe specific performance targets, Meta maintains that asking providers to set a specific response time, even if just in target form, does not account for the necessary nuance in assessing cases with differing levels of complexity which may require complex rights-balancing assessments nor does it account for the complexity of at-scale content moderation systems which aim to prioritise the review and removal of a variety of types of violating content against a range of factors e.g. virality, severity. Indeed, even in a given "violation" category, no two violations are the same, so it is not practicable to set a single target turnaround time for a given category, let alone a single turnaround time for a reporting and flagging mechanism as a whole.

Requiring providers to set and comply with turnaround targets has a real potential to create a blunt solution with unintended consequences and/or incentives, and reduce the efficacy of report/flagging handling. In particular, it may serve to disincentivise providers from taking the necessary time to properly consider the more complex issues that could be raised and it may lead to underenforcement or overenforcement, with negative impact to free speech.

In addition this measure 4C (Setting internal performance target) conflicts with measure 4D (priorisation, see below), as when priorisation applies when content would be reviewed would be a fluid state dependent on the current priorisation queue.

b) Moreover, it is unclear how accuracy in decision making is to be defined and assessed. For instance, would a decision be considered accurate if it's not appealed? Would it be considered accurate if it's appealed and the content is restored? These are complex decision making processes in areas where there are a wide variety of different applications and outcomes.

c) In contrast, taking an approach that does not involve setting prescriptive internal performance or accuracy targets, but that rather emphasises the general requirement for content to be reviewed swiftly, aligns with other regulations, such as the DSA.

To this end, we strongly advise against including this requirement in the draft CoP. To the extent Ofcom decides to maintain the internal target proposals, we suggest further guidance by Ofcom particularly with regard to how such targets should operate as against other signals guiding prioritisation in content moderation systems.

4. All 'multi-risk' or large U2U services: Prioritisation (ref 4D)

Per this measure Ofcom recommends that "*the provider should prepare and apply a policy in respect of the prioritisation of content for review. In setting the policy, the provider should have regard to at least the following:*
a) the virality of content: the provider should prioritise content for review in a way which minimises circumstances in which the number of users encountering a particular item of illegal content increases exponentially over a period of time;
b) the potential severity of content: including whether the content is suspected to be priority illegal content and the risk assessment of the service; and
c) the likelihood that content is illegal content, including whether it has been reported by a trusted flagger."

For review whether content violates provider policies we support the criteria of "virality" and "severity" in application as above, but, we also recognise there are significant and concerning practical implications as to the details of these factors, the remainder of Ofcom's proposed factors, the interplay of the factors, applying these factors to review of content for illegality, and conflicts with other proposed measures. In detail:

Most providers' global policies, for the reasons outlined in our response (e.g. Question 49), do not precisely overlap with all forms of locally illegal content. This is relevant for two reasons:

- Measure 4D proposes that, when having regard to the potential severity of content, the provider should take into account "*whether the content is suspected to be priority illegal content and the risk assessment of the service*". Given that we would in the first instance be assessing content for violations of our policies, not for illegality, it would not be practical to prioritise on the basis of illegality and the results of our illegal content risk assessment. Such policy review as a first step has advantages, as in case content is assessed as policy violating it would be removed globally instead of a local restriction. We suggest that the measure instead gives providers the flexibility to assess severity in a way that works for their moderation process which often operate most effectively at a global scale (as the underlying systems can continually evolve and be trained on a larger set of content and data). Providers may e.g. prioritise in their content moderation on content that violates their policies suspected content violating policies in the field of CSEA and terrorism.

- Measure 4D also proposes that the provider's prioritisation should take into account "the

likelihood that content is illegal content, including whether it has been reported by a trusted flagger". It would not be practical for us to take into account the likelihood of content being illegal, for the same reasons set out above. We suggest that the measure instead gives providers the flexibility to prioritise on other grounds aside from illegality - for example, the likelihood that content violates their policies. In any event, where reports from trusted flaggers are concerned, in most cases those reports are processed via separate, dedicated channels that don't operate in tandem with content moderation systems.

We are also concerned that the prescriptive nature of the current measure would cause additional practical issues:

- Certain priorisation parameters are conflicting - for example, the measure indicates that reports being received from a trusted flagger goes to their likelihood of illegality, but a trusted flagger may report lower severity content which should not be prioritised over higher severity content reported by an ordinary user. Similarly, it may at times be appropriate to prioritise highly viral content that does not appear to be priority illegal content over content that is alleged to be priority illegal content but that is being encountered by very few users. Providers should have the flexibility to prioritise in a way that works for their platform and moderation processes, and the types of content they are most likely to encounter.

- In addition, we note that a consultation planned for Q2 2024 will cover guidance for child safety duties, which will include dealing with content that is not illegal. We are concerned that prioritisation on the basis of illegality, as covered in measure 4D, may conflict with guidance on prioritisation for other types of legal content and / or result in the handling of such content being deprioritised. Allowing greater flexibility for providers in relation to prioritisation would mean that these considerations could be balanced by providers in a way that is effective for their services, rather than prescribing an approach to prioritisation that may have unintended consequences.

<u>We therefore suggest that providers are granted flexibility to prioritise in a way that is appropriate for their service and in light of a wider range of relevant factors, and that any more prescriptive requirements are introduced at a later point, once all relevant consultations have been completed.</u>

<u>5. All 'multi-risk' and large U2U services: Resourcing (ref 4E)</u>

Per this measure *"the provider should resource its content moderation function so as to give effect to its internal content policies and performance targets having regard to at least:*
a) the propensity for external events to lead to a significant increase in demand for content moderation on the service; and
b) the particular needs of its United Kingdom user base as identified in its risk assessment, in relation to languages."

We agree with the goal of ensuring appropriate resourcing, including adaptability under changing circumstances, and we agree in general with Ofcom's proposal.

We refer to our response to proposed measures 4B and 4C above, where we comment on the proposed measures regarding internal content policies and performance targets that are referred to in this measure.

In addition, we stress that the implementation of this measure in practice needs to be proportionate. For example: it is reasonable for providers to have appropriate backup strategies for unexpected surges in report volume, but even with such strategies in place, not every eventuality can be planned for, and some situations may require additional ad hoc measures that will take time to implement. Also, while we agree with the goal to have appropriate resourcing in place and cater for particular needs of a UK user base, we also stress that the correct staffing of language support worldwide is a complex planning exercise; even on a per region level depending on the amount of languages spoken in the region.

Based on our experience we set out below strategies that we have found helpful, which Ofcom may wish to consider reflecting in the measure:

- Using a mix of reviewers: We use reviewers from a variety of different backgrounds, to cater for appropriate language support and understanding of cultural context. However, for languages that are widely spoken in the world, like English, it is helpful to have content moderation teams that provide global coverage, which enables the provider to quickly redeploy capacity if there is a surge in demand in a specific country, in times of crisis, or when unpredictable events occur. This means it is helpful to have the option to rely temporarily on teams that provide global coverage to mitigate more local risks.
- Allowing for triaging where more or less language support is needed: Language expertise helps to e.g. enforce policies in cases where certain words or content require additional contextual understanding, but not all content requires language expertise. For example, some nudity and sexual activity is language agnostic. For this type of content, it is helpful to have a global pool of content moderators who review these types of reports.

6. All 'multi-risk' or large U2U services: Provision of training and materials to moderators (ref 4F)

"The provider should ensure people working in content moderation receive training and materials that enable them to moderate content in accordance with Recommendations 4A and 4B. This measure does not apply in relation to volunteers.
The provider should ensure that in doing so:
a) it has regard to at least the risk assessment of the service and information pertaining to the tracking of signals of emerging illegal harm; and
b) where the provider identifies a gap in moderators' understanding of a specific kind of illegal harm, it gives training and materials to remedy this."

We support Ofcom's recommendation to ensure moderators are appropriately equipped. To that end we support appropriate measures, such as distinct training based on the nature of the particular moderator's work.

We refer to our responses above regarding measures 4A and 4B, which are referred to in measure 4F.

In addition, we stress that the implementation of this measure in practice should be proportionate to achieve its purpose. As outlined in our response (see our responses to Questions 8 and 49), the content prohibited by providers' policies is not necessarily identical to the types of illegal content covered by the OSA. Given this, where content moderators work on reviewing content for violation of the provider's policies, they should receive training on such policies. This may cover content that to some extent overlaps with particular kinds of illegal harm, but will not necessarily cover all forms of illegal harm. Conversely, content moderators who review content to determine whether it constitutes a specific kind of illegal harm should receive training on such harm. For the latter, providers should have flexibility to implement illegal harm-specific training in a way that is

appropriate for their service and reflective of the particular risks of illegal harm that apply to their service. Based on our experience, we set out below strategies that we have found helpful, which Ofcom may wish to consider reflecting in the measure: ● Building review teams for policy violations that include a diverse range of backgrounds, and that include experts in enforcement in policy areas such as counter terrorism and child safety. Review teams should undergo initial training to ensure that they have a strong grasp on policies, and should be trained and tested as appropriate beyond this initial training. ● Human reviewers who review content alleged to be illegal receive distinct training based on the particular nature of their work. This includes training on operational proficiency and preparation for processing such content. For example, the reviewers who review content for defamation receive training specifically on assessing defamation.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 18 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Content moderation (Search)

Question 19: **Response by Meta**
i) Do you agree with our proposals?
Response: We understand this Question refers not to user to user services, but to search services. On that basis, we have no comment
ii) Please provide the underlying arguments and evidence that support your views.
Response: As above (Question 19(i))
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Automated content moderation (Search)

Question 27: **Response by Meta**
i) Do you agree with our proposals?

Response: We understand this Question refers not to user to user services, but to search services. On that basis, we have no comment.
ii) Please provide the underlying arguments and evidence that support your views.
Response: As above (Question 27(i))
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

User reporting and complaints (U2U and search)

Question 28: **Response by Meta**
i) Do you agree with our proposals?
Response: We understand this Question refers to the recommended measures 5A to 5I in Annex 7 of the consultation, which relate to the OSA requirements to have easy-to-use reporting and complaints processes that allow users to report relevant types of content (e.g. illegal content) and make relevant types of complaints, and to take appropriate action in response to complaints. We note that while the OSA separately addresses reports (s. 20) and complaints (s. 21) there is some overlap between these provisions, and Volume 4 and Annex 7 often use the term 'complaints' to refer to both. Our response below covers both reports and complaints. Our comments on these proposals are as follows: 1. We support Ofcom's view that services could operate a combined reporting and complaints function for most users and most types of complaints, provided that there is at least one other means for users to communicate these issues to the service, so that complaints can be made about issues with the reporting function itself (Volume 4, paras 16.15-16.16). 2. The measures set out at 4A to 4F in Annex 7, which we address in our response to Question 18 above, include measures relating to the handling of user reports and complaints. The comments we set out in relation to those measures are also relevant here - for example, our comments above in relation to proposed internal targets and turnaround times apply similarly to the measures recommended at 5C, 5D and 5E, as these relate to timelines and the taking of appropriate action in response to complaints. 3. In relation to measure 5B, which proposes that "for relevant complaints regarding a specific piece of content, a reporting function or tool is *clearly accessible* in relation to that content", we agree that reporting functions should be clearly accessible, but there is a practical question about how this would work in relation to "affected persons".

The OSA requires affected persons to be able to make reports and complaints, per sections 20 and 21. In s. 10(5) OSA, an affected person is defined as covering persons "other than a user of the service in question" who fall within certain categories - i.e., affected persons are not users.

We note that providers do not necessarily allow non-users access to all content on their services - for example, some providers have limits in place on how many pieces of content a non-user can see, have settings where users can choose whether their content is visible to everyone or just their "friends" or do not permit sharing of content with non-users. This is generally done for reasons of safety and user privacy - for example, to mitigate the risk of data scraping by non-users, give users control over who can see their content, or to prevent people who are not participating in a private chat from viewing messages sent in the chat (as this would mean the chat was no longer private).

As such, affected persons will not necessarily be able to see an item of content that they may wish to report or complain about, and so may not be able to access a reporting / complaint tool directly from that content. We therefore strongly suggest that 'accessible' functions and tools for reporting / complaints are not limited to those accessible directly from the relevant item of content, but are deemed to include other functions and tools accessible to non-users - for example, reporting by way of a Help Center form.

We also note that other elements of measure 5B, e.g. the recommendation that "the number of steps necessary (such as the number of clicks or navigation points) to submit (i) a relevant complaint using the reporting function or tool; and (ii) any other kind of relevant complaint are as few as is reasonably practicable", will need to be interpreted flexibly to account for differences between services and different ways services can be accessed. For example, the space available on the user surface of a mobile phone app is likely to be more limited than the user surface of the same service accessed via a desktop browser, and users may be used to finding reporting options in different places depending on how they access the service. It would therefore be important for providers to have flexibility in how they meet this recommendation, to account for differences between services and between different methods of access to a service.

4. For measure 5C, which recommends that providers "acknowledge receipt of each relevant complaint and provide the complainant with an indicative timeframe for deciding the complaint", we highlight two practical challenges.

   Firstly, service providers regularly encounter users or non-users who abuse the reporting system by "spamming" high volumes of reports with no merit or submitting coordinated bot reports, and act to the detriment of those genuinely reporting harmful or illegal content. We suggest that measure 5C should include an exception for reports identified as spam, to reduce the resource impact for providers of dealing with such reports and allow more resources to be dedicated to dealing with legitimate reports. There are objective criteria that may be used to identify spam reports, which we are happy to discuss with Ofcom separately (we have not set these criteria out in this public response, in order to prevent misuse by bad actors).

   Secondly, as regards the proposal for indicative time frames for sharing a response, we note that it is likely to be difficult to provide even an indicative timeframe for responding to reports / complaints, as the time needed for a proper assessment and response will be highly variable and is often difficult to identify before having reviewed the report /

complaint. For example, the prioritisation and timeline of review for various types of reports cannot happen instantaneously as it depends on multiple factors within the content moderation system including how other content is to be prioritised against other reported content in a prioritisation "queue" or system.

While we appreciate Ofcom's clarification in Volume 4 para. 16.101 that these timeframes are not binding deadlines, we are concerned that providing users with timeframes on submission of their report / complaint, which timeframes may not subsequently be met, will lead to more frustration for users and incentivise providers to respond faster (at the expense of appropriate prioritisation and proper assessment of the report / complaint) in order to stay close to the indicated timeframe. See our comments in response to Question 18 regarding internal performance targets, which apply similarly here.

In addition, an indicative time frame does not align with the proposed measure 4D for prioritisation. Prioritisation is an ongoing process, the response time for a report would then vary depending on what reports/complaints come in, e.g. an initial estimate may be overhauled a few minutes later when reports with higher priority or, for example, when particular spikes occur during certain high profile events or incidents come in and which may be hard to plan for.

We also note, with reference to Ofcom's aim of harmonising with other content regulations, that the DSA does not include an equivalent requirement of indicative time frames.

5. Measure 5I includes a proposal for large services and those at medium or high risk of fraud to set out a dedicated policy to set up a reporting channel for certain trusted flaggers.

   While we understand the aim of this proposal, we note that providers may already have dedicated reporting channels for trusted flaggers, which enable a range of reports, including fraud-related reports. For example, Meta has existing, dedicated reporting channels where government agencies and non-governmental organisations can report harmful or illegal content on Facebook or Instagram that may violate our terms and policies or that they consider to be in breach of local law, including fraud. These reporting channels are distinct from standard in-product reporting (which is open to all users), can only be used by the onboarded organisations, and are staffed by escalations specialists who triage reports and route them to expert teams for expedited analysis, including more in-depth investigations where appropriate. Some of the recommended trusted flaggers by Ofcom are already onboarded to our dedicated channels and use this process. Where such channels already exist, we would question the need for providers to set up a second and separate channel dedicated to fraud reports. This is all the more relevant given that when content is reported to our teams via dedicated channels for trusted flaggers, content is not merely reviewed against one specific policy area but across all potentially applicable terms/policy violation types. Such an approach would be hampered by the existence of a separate, distinct channel.

   In addition, we note that where a provider has a reporting channel for a wider range of trusted flaggers than those listed in the measure, it may not be practical for the provider to commit to engaging with all of those organisations to understand their needs with respect to the channel. While we appreciate that Ofcom's recommended measure only refers to such engagement with reference to the seven trusted flaggers listed in the

measure, we propose that providers should have the flexibility to limit such engagement to these organisations, rather than providers being required to engage with all organisations onboarded as trusted flaggers. This could be clarified in the wording of the measure.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 28 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Terms of service and Publicly Available Statements

Question 29: **Response by Meta**
i) Do you agree with our proposals?
Response: These measures, which reflect the OSA's terms of service ('ToS') provisions, require extensive information to be included in the ToS. Our experience suggests that providers should have the flexibility to put this information in separate documents or locations (which are incorporated into the ToS by reference) in order to improve readability and clarity for users. Meta takes great care to ensure that all of its communications with users, including its terms and conditions, and any updates or changes thereto, are set out in clear, plain, intelligible, user-friendly language for users of all ages. In this context, we believe that terms of service should remain short and clear.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 29 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 30: **Response by Meta**
i) Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response: We have no comment on this.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We have no comment on this.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Default settings and user support for child users (U2U)

Question 31: **Response by Meta**
i) Do you agree with our proposals?
Response: In general, we agree with the proposal that by default enabling stricter privacy protecting options improves the safety of teen users on services. However, different protective measures may be appropriate for different services, depending on the nature, risks and user base of the service, and we would advocate for providers to have flexibility in deciding which protective measures to adopt in order to account for these differences. Additional flexibility would also allow providers to implement protections in a way that takes account of their existing safety measures (which will be particularly important for providers who have already invested substantially in protections for child users) and will allow protections to evolve as necessary to reflect the fast pace of change in children's experience online. We therefore propose that Ofcom provides additional examples of recommended measures that will give providers greater flexibility to adopt protections that work for their service while remaining within the COPs 'safe harbour'. For context, and as examples of measures that providers may take to protect teen users of their services, we refer to these previous articles (Facebook private settings, Instagram private by default) and this very recent article on message settings for teens on Facebook and Instagram, which outline examples of default settings and other protective measures that we have implemented in the past, and most recently for teen users on Facebook and Instagram. In our experience, these measures are geared towards achieving the same goals targeted by Ofcom's recommended measures (i.e., to reduce the risk that teen users might inadvertently be exposed to inappropriate interactions and content which could result in grooming). We think that the measures we have taken so far are proportionate to mitigate this risk for these services, but we continue to monitor this and adjust these measures to reflect developments on our platforms.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 31 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 32: **Response by Meta**

i) Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response: We have no further comment.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 33: **Response by Meta**
i) Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response: We have no further comment.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Recommender system testing (U2U)

Question 34: **Response by Meta**
i) Do you agree with our proposals?
Response: While we have robust systems in place to ensure the integrity of our recommender systems, we would suggest avoiding setting prescriptive requirements in the CoPs, especially if they apply only to providers that are already testing their systems. This would have the opposite effect of that intended, by encouraging providers which did not invest in this space to continue to do so to avoid regulatory pressure. We would recommend that providers are given flexibility as to how they approach recommender systems development and testing, and - in particular - that providers are able to use different strategies to detect and address changes in prevalence in harmful content that may stem from ranking changes, without thereby falling outside the CoPs 'safe harbour' (rather than being limited to a launch-by-launch AB test approach if they wish to remain within the 'safe harbour').
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 34 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 35: **Response by Meta**
i) What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response: We have no comment.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Service design and user support (Search)

Question 44: **Response by Meta**
i) Do you agree with our proposals?
Response: We understand this Question refers not to user-to-user services, but to search services. On that basis, we have no comment.
ii) Please provide the underlying arguments and evidence that support your views.
Response: As above (Question 44 (i))
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Cumulative Assessment

Question 45: **Response by Meta**
i) Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response: We have no comment.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We have no comment.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 46:

Response by Meta
i) Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response: We have no comment.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We have no comment.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 47: **Response by Meta**
i) We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response: As discussed in our response to Question 13 the draft CoPs set out a 'differentiated' approach to apply the most onerous measures in the proposed CoPs only to services which are large and/or medium or high risk. As mentioned, while we believe there is merit in varying recommended measures to take account of the varying risks and capabilities of different services, we do not believe that high reach services are automatically more risky for users per se, and hence it would be disproportionate to impose obligations only on the basis of size. We refer to our feedback on Questions 12 to 16.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 47 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Statutory Tests

Question 48: **Response by Meta**
i) Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?
Response: We have no further comment.
ii) Please provide the underlying arguments and evidence that support your views.

Response: We have no further comment.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Volume 5: How to judge whether content is illegal or not?

The Illegal Content Judgements Guidance (ICJG)

Question 49: **Response by Meta**
i) Do you agree with our proposals, including the detail of the drafting?
Response: *On the two options Ofcom lays out to fulfil the obligation to address allegedly illegal content - Option 1 to review reported content for illegality on a case-by-case basis (where necessary) and based on the alleged local law violations and Option 2 amending the ToS in a way that they would cover all possible UK offences* We appreciate that Ofcom suggests two approaches to providers to fulfil this obligation under UK law, and we propose to adopt the first approach. Due to our global scale and international regulatory commitments, we've developed both a robust set of policies to address a wide variety of harmful content and a comprehensive process for reviewing reports alleging that content on Facebook or Instagram goes against local law. What is illegal varies per country, whereas our policies set a global baseline. While there is often a large overlap between content that could go against our policies and content that could violate local law (including UK law), our policies are neither intended to nor could they match every country's law. When we introduce one country's standard for illegality at a global scale, this may contradict another country's standard. In this context i.e. where an individual wishes to report content as falling foul of local law, we consider a multi-step approach sensible. We first review content reported for alleged illegality against our policies, e.g. Facebook Community Standard or Instagram Community Guidelines. If such content goes against our policies, the content is removed globally for all users. If content reported for alleged illegality does not go against our policies, in line with our commitments as a member of the Global Network Initiative and our Corporate Human Rights Policy, we conduct a careful legal review to consider whether the request is procedurally valid and whether the content violates local law. In some instances, this is followed by human rights due diligence. Where we act against content on the basis of local law, we restrict access to the content in the jurisdiction where it is alleged to be unlawful. For completeness sake, it is worth noting that

while some assessments of content can be done quickly e.g. within hours, other cases can take days to assess. This is often only apparent once we have initially reviewed the report and is not possible to estimate up front.

We have adopted this model because, according to international human rights law, any restriction on content must be implemented by the least restrictive means. We assess the request and our enforcement options to ensure any action taken on the content is done in the most narrow and specific way possible taking into account the product, tooling capabilities, and any temporal nature of the legal obligation.

Clarity

We welcome some of the clarity provided by the Illegal Content Judgement Guidance (ICJG) draft with regard to some specific offences. We consider the ICJG to be one of various (legal) sources that we can refer to when making judgements about the illegality of content.

Assessing Intent

We appreciate the acknowledgement of the difficulties in assessing inferences about the state of mind of the reported user sharing allegedly illegal content. Therefore, we advocate for only including clear contextual signals in the legality assessment - for example, the way in which the content has been shared (e.g. adding a caption to a previously shared video, addressing another user by directly responding to that user's content).

In relation to inferring conduct, behaviour and state of mind when content has been posted by a "bot", we note that this will come with particular practical and technical challenges for the content reviewer to have sufficient signal to make these inferences and to identify the person who is (or is assumed to be) controlling a "bot".

Level of detail

We welcome the ICJG's provision of comprehensive guidance on specific offences and their requirements. While we believe the guidance brings the right level of details at this stage, given that this is a very dynamic space, we think that additional guidance from Ofcom may be helpful once the new regime is in force and we have a better understanding of the complexities we will face in practice regarding illegal content judgements. We would also find it helpful if Ofcom could clarify how it expects providers to deal with offences not currently included in the ICJG.

Malicious reporting

Regarding the suggestion to take into account potential malicious reporting in the legality assessment, we would appreciate more clarity as to what extent the existence of several reports (with malicious intent) could/should be part of this assessment. In our view, the fact that a specific piece of content has been reported more than once does not change the approach of the legality assessment, as this is based on the relevant legal provision.

Further, we would like to highlight that our policies allow us to enforce against a broad range of violating behaviours: actor-based enforcement, which involves the removal of accounts because of the totality of their activity on the platform; behaviour-based enforcement, which is predicated on specific violating behaviours exhibited by violating actors; and content-based enforcement, which predicates enforcement on specific violations of our Community Standards. In this context, what Ofcom calls out as malicious reporting could qualify under our dedicated policies tackling abusive activities and behaviours (such as spam, inauthentic behaviour, coordinating harm etc.) which would trigger specific restrictions on the accounts. To the extent regulatory harmonisation is feasible, we would also note the DSA's provisions on abusive user reporting practices.
ii) What are the underlying arguments and evidence that inform your view?
Response: Please see our response to Question 49 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 50: **Response by Meta**
i) Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response: We have no comment.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We have no comment.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 51: **Response by Meta**
i) What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response: Although we generally agree that ideally, what information is considered to be reasonably available and relevant to illegal content judgements would be the same across all services, we would advocate for an approach that takes into account the technical specifics of different services. In our view, "reasonably available information" should not be too broadly defined and should be also limited to information that may also be relevant rather than merely "reasonably available". Providers need to balance the pursuit of users' safety with other considerations, such as the

protection of users' privacy. In this context, accessing additional information beyond the specifically reported piece of content or its context (such as other account information of the reported user) could cause imbalance. In addition, due to our global scale, the volume of content for review is such that it would be disproportionate to require global providers to collect superfluous information to make an assessment. In addition, to ensure the integrity of the platform and our processes, we would always advocate for a harmonised approach with other content regulation for the review process at scale.

Due to the technical functionalities of the different services, there may also be circumstances where the level of information available may vary. We would therefore advocate for an approach which allows providers to take into account the specifics of the respective service.

As mentioned in our response to Question 49, our policies cover the three dimensions of online safety and integrity: actors, behaviours and content and as such we have dedicated and specific enforcement actions against harmful activities and behaviours.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:
Response by Meta

i) Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?

Response:

Meta welcomes the explanation of Ofcom's proposed approach to the exercise of its information gathering powers as outlined in Volume 6. However, there are some areas that Meta considers would benefit from further refinement or clarification, as outlined below.

Meta notes that Ofcom has confirmed that it "*expect[s] to publish guidance on how we will use our information gathering powers at a later stage in the implementation of the Act*" (the "**Information Gathering Guidance**"). Meta suggests that many of the points it raises in this response can be clarified in the Information Gathering Guidance.

Information notices

Meta welcomes Ofcom's statement that it will, where appropriate, send information notices in draft form.[1] Meta believes that this should be the standard, default approach when sending information notices to service providers, and should only be departed from in exceptional circumstances. Sharing information notices in draft form will allow Ofcom and the relevant service provider to engage constructively on the scope of the requests and any issues the provider may face in responding (for example, data not being available in the requested form, or difficulties producing the requested information within the specified timeframe) and agree, for instance, changes to the language of the request or the production of certain information in different phases. It will allow these discussions to take place upfront, rather than having to be negotiated after a finalised information notice is issued when the service provider will also be working to respond to the information notice in the specified time frame.

Meta therefore suggests that the Information Gathering Guidance (and / or other Ofcom guidance) should clarify the circumstances in which Ofcom will issue information notices in draft form including (if Ofcom agrees with the position outlined above):

- that its standard approach will be to issue information notices in draft form; and
- the circumstances in which it will deviate from this standard approach (for example, where there is exceptional urgency to gather the required information).

Remote viewing powers

Meta notes that, as part of its information gathering powers, Ofcom can require that a service provider enables Ofcom to remotely view: (i) information demonstrating in real time the operation of systems, processes and features used by the service; and (ii) information generated in real time by the performance of a test or demonstration (the "**Remote Viewing Powers**").[2] Meta's view is that the Remote Viewing Powers are an intrusive measure, which would likely require significant resources from the service provider.

Ofcom has confirmed that it does not intend to use the Remote Viewing Powers "*as often as its information notice powers*".[3] However, in line with Ofcom's regulatory principle to seek the least intrusive regulatory methods of achieving its objectives,[4] and its duty to exercise its power to require information in a way that is proportionate under s. 100(4) OSA, Meta is of the view that the Guidance should explicitly state that these Remote Viewing Powers should be reserved for more serious or complex cases. This is consistent with the approach Ofcom intends to adopt to the exercise of its power to require skilled persons reports, and powers of entry, inspection and audit (see also below).[5]

Meta also considers that Ofcom should not use its Remote Viewing Powers as the first step in any information gathering process, given Ofcom's ability to utilise other, less-intrusive information gathering tools, and should make clear that this is its intention either in guidance or in other public documentation.

---

1 Volume 6, paragraph 28.51.

2 Volume 6, paragraph 28.9.

3 Volume 6, footnote 6.

4 Volume 6, paragraph 28.49.

5 Volume 6, paragraph 28.52.

Meta would welcome further guidance in the Information Gathering Guidance (and / or other Ofcom Guidance) on the circumstances in which Ofcom intends to use the Remote Viewing Powers including (if Ofcom agrees with the position outlined above) clarification that:

- Ofcom intends to use the Remote Viewing Powers only in more serious or complex cases; the Remote Viewing Powers will not be used as the first step in an initial information gathering exercise, rather will only be used where (for example) the responses to an initial information notice were not satisfactory;
- consistent with the approach to information notices, the standard approach will be to issue any Remote Viewing Powers requests in draft form, for the reasons set out above; and
- Wherever possible, Ofcom will use the Remote Viewing Powers only with respect to test data, in a sandbox environment.

Other information gathering powers

As noted above, Ofcom has stated that other information gathering powers such as skilled persons reports and powers of entry, inspection and audit "will typically be reserved for more serious or complex cases".[6] Meta welcomes this proportionate approach. However, Volume 6 does not include further information on how "seriousness" will be assessed when Ofcom decides whether to make use of these information gathering powers.

Meta would welcome further guidance in the Information Gathering Guidance (and / or other Ofcom Guidance) on the meaning of "serious" in this context, including examples of where Ofcom considers the use of these powers to be appropriate because the case is sufficiently serious or complex. Seriousness could be assessed by reference to a number of different factors – for example, the alleged conduct of the service provider (including whether there is an element of intention or recklessness), or the degree of actual or potential harm caused by the alleged conduct.

Senior manager requirement

Meta notes that Ofcom may require a service provider to name a relevant senior manager who may reasonably be expected to be in a position to ensure that the service provider complies with the requirements of an information notice (the "**Senior Manager Requirement**").[7] The senior manager named in an information notice faces criminal liability if: (i) the service provider fails to comply with an information notice; and (ii) the senior manager fails to take all reasonable steps to prevent the failure.[8]

Meta recognises that requiring a service provider to name a senior manager to be responsible for the response to an information notice may, in certain limited circumstances, be a legitimate way of incentivising compliance by service providers who might otherwise be unlikely to comply or unlikely to comply fully. However, the Senior Manager Requirement would impose a disproportionate burden on service providers to identify the appropriate senior manager for each information notice if used as a matter of course. It is also one of the most severe powers available to Ofcom in its information gathering capacity, given that it could ultimately result in a criminal conviction (including a fine or even imprisonment) for the named senior manager.

[6] Volume 6, paragraph 28.52.

[7] Volume 6, paragraph 28.16; paragraph A5.37, Annex 11.

[8] S. 110 OSA.

In terms of the burden on service providers, in reality, each information notice is likely to require information that will span the remit of many senior individuals at a service provider: meaning that it will be artificial for the service provider to nominate a single individual as being responsible for complying with any information notice. Given the significant (criminal) consequences for the individual ultimately nominated, the process of a service provider identifying who is the right person to bear this risk is likely to require careful consideration and structuring and would not, ultimately, fulfil the intended purpose of the nomination requirement.

Meta therefore considers that, in line with Ofcom's regulatory principle of proportionality, the Senior Manager Requirement should not be used as a matter of course in every information notice issued by Ofcom Rather, the use of this power should be limited to circumstances where Ofcom has evidence based concerns that the service provider will not adequately comply with the information notice without such a requirement being imposed. This could be based, for instance, on past incidents of the service provider failing to provide adequate responses to information requirements.

Meta would welcome further guidance in the Information Gathering Guidance (and / or other Ofcom Guidance) on the circumstances in which Ofcom intends to use the Senior Manager Requirement. If Ofcom agrees with the position outlined above, this should include clarification that Ofcom will only use this power if it has concerns that the service provider will not adequately comply with the information notice without such a requirement being imposed, and examples of the types of the situations where this concern may arise.

Skilled person

Paragraph 28.24 of Volume 6 reflects s. 104 OSA which confers on Ofcom the power to: (i) appoint a skilled person; and / or (ii) require a service provider to appoint a skilled person (the "**Skilled Person Power**").

Whilst Meta acknowledges that the two alternatives are the product of legislation, Meta is of the view that the default position should be that Ofcom requires the *service provider* to appoint a skilled person, rather than Ofcom appointing a skilled person itself.

The purpose of a skilled person is to: (i) assist Ofcom to identify and assess non-compliance, or potential non-compliance, of a service provider; and / or (ii) develop Ofcom's understanding of the nature and level of risk of a service provider not complying with its obligations and ways to mitigate such a risk. Given the technical nature of this work, and the need for the skilled person to analyse and understand a service provider's systems, it follows that the relevant service provider will, in most cases, be best placed to identify the candidate with the requisite knowledge and expertise to carry out the skilled person's role. This should be the default position save for exceptional circumstances, for example where Ofcom has valid concerns about how the provider would comply with its direction to appoint a skilled person (i.e. by failing to appoint a candidate, or appointing a candidate who is clearly unsuitable for the role).

Meta would welcome further guidance in the Information Gathering Guidance (and / or other Ofcom Guidance) on the circumstances in which Ofcom intends to use the Skilled Person Power. If Ofcom agrees with the position outlined above, this should include clarification that Ofcom will ordinarily require the service provider to appoint a skilled person save for in exceptional circumstances, including examples of those exceptional circumstances. Other additional

information that Meta would welcome further guidance on in relation to Ofcom's exercise of its Skilled Person Power include:

- the specific purposes for which Ofcom may appoint a skilled person as a supervisory tool,[9] as well as a non-exhaustive list of examples of how the power may be used in relation to each of these specific purposes;[10]
- the factors Ofcom will take into account when deciding whether to appoint a skilled person, including circumstances relating to the firm, alternative tools available (including other statutory powers), legal and procedural considerations, the objectives of the enquiries, costs considerations (see below) and considerations relating to regulatory resources;[11]
- the criteria the skilled person must meet to be appointed or approved by Ofcom;[12] and
- the level and payment of a skilled person's fees, including whether Ofcom will take into account the potential cost of a skilled person's engagement when considering whether to order the appointment of a skilled person.

Meta notes, by way of example, that the Financial Conduct Authority (the "**FCA**") has published detailed guidance on the use of skilled person reports in a financial services context (see chapter 5 of the FCA's Supervision Manual ("**SUP**") and the Use of Skilled Persons Part of the PRA Rulebook). By way of example, we have identified the relevant sections of SUP which cover the topics outlined at sub-paragraphs 1.15.1 to 1.15.4 above in the relevant footnotes.

Ofcom's proposed approach to supervision

Meta notes that Ofcom has not specifically requested feedback in relation to Chapter 30 of Volume 6; however, Meta nevertheless wanted to take this opportunity to comment on Ofcom's proposed approach to supervision.

Meta welcomes Ofcom's indication that its approach to supervision will be flexible, proactive, proportionate and risk based and will focus on the effectiveness of service providers' systems and processes protecting their users, not on individual pieces of content.[13]

Meta further welcomes Ofcom's stated objective of seeking to resolve issues constructively with service providers, without pursuing formal enforcement action, as this can provide the quickest and most efficient route to ensuring users are protected from harm.[14] Meta is confident that this collaborative approach to supervision will help Ofcom develop a better understanding of the way service providers operate and drive improvements in user safety.

Meta also supports Ofcom's indication that issues will only be passed from the Supervision to the Enforcement teams in circumstances where Ofcom has serious compliance concerns about the service provider, and the service provider is unwilling to engage with Ofcom in a constructive manner.[15]

---

[9] SUP 5.3.1G.

[10] SUP 5.3.1.AG.

[11] SUP 5.3.

[12] SUP 5.4.8G.

[13] Volume 6, paragraph 30.5.

[14] Volume 6, paragraph 30.22.

[15] Volume 6, paragraph 30.23.

Meta would welcome more guidance on:

- the framework or criteria that the Supervision team intends to use to decide when to refer issues to the Enforcement team;
- what Ofcom considers to be a "*constructive*" form of engagement should compliance concerns be identified; and
- whether Ofcom intends to communicate such compliance concerns and concerns over whether the engagement is "constructive" and provide the opportunity for remediation prior to any referral to enforcement.

ii) Please provide the underlying arguments and evidence that support your views.

Response: Please see our response to Question 52 (i).

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Enforcement powers

Question 53:
Response by Meta

i) Do you have any comments on our draft Online Safety Enforcement Guidance?

Response:

Meta welcomes the explanation of Ofcom's proposed approach to the exercise of its enforcement powers as outlined in Volume 6, and the draft Online Safety Enforcement Guidance in Annex 11 (the "**Draft Enforcement Guidance**"). However, there are some areas that Meta considers would benefit from further refinement / clarity, as outlined below.

Proposed approach to online safety enforcement

Meta is committed to continuing to improve its systems and processes and engaging with Ofcom as the industry works to reach full compliance with its duties, including the illegal content and child safety duties, under the OSA. Meta therefore welcomes Ofcom's pragmatic acknowledgment that service providers may require a reasonable period to put in place appropriate systems and processes to bring them into full compliance with their illegal content and child safety duties, as well as its indication that it will prioritise only serious breaches of these duties for enforcement in the early stage of the regime.[16]

Meta also welcomes Ofcom's indication that it will not take enforcement action based solely on evidence of isolated instances of harmful content appearing on a service; the focus instead being on the service provider's systems and processes.[17] However, should Ofcom proceed with its proposals to engage with complainants throughout the initial assessment and enforcement process, Meta considers that Ofcom should more clearly state that it does not ordinarily intend to enforce against single pieces of harmful content in parts of the Draft Enforcement Guidance which

[16] Volume 6, paragraphs 29.12 – 29.14.

[17] Annex 11 paragraph A3.6.

relate to complainants (for example at Annex 11, paragraphs A4.9 – A4.10 and A4.12). This is important because complainants are more likely to focus on single instances of harmful content, without specific consideration of, or visibility over, whether such content constitutes systemic failures on the part of the service provider.

Initial assessment

Evidence required for commencement of Ofcom's investigation

The Draft Enforcement Guidance provides that where Ofcom identifies potential compliance concerns, it will assess the issue and consider whether it is appropriate to open an investigation or take some other action. This will be done on a case-by-case basis.[18] It would be helpful for Ofcom to clarify what kind of evidence would be required for an investigation to be triggered, for instance by providing examples in the Enforcement Guidance. In line with Ofcom's overarching objective to take a reasonable and proportionate approach to enforcement, and to allow Ofcom to effectively prioritise the most serious breaches of duties by service providers, Meta considers that this evidential bar should be high, especially given Ofcom's current intention to publicise the opening of an investigation.

Engagement with the service provider during initial assessment

Ofcom states that it may engage with the service provider as part of the initial assessment to give the service provider an opportunity to comment on the issue(s) and provide information to assist Ofcom in determining what action, if any, should be taken.[19] Meta supports this proposition and considers that Ofcom should adopt this approach in every case, save for exceptional circumstances. Treating engagement with the service provider as a necessary aspect of initial assessment will allow Ofcom to gain a better understanding of the issue and the service provider's perspective. It will also enable Ofcom to make a more informed decision about what enforcement action, if any, should be taken and ensure that such action is reasonable and proportionate to the issue (and supported by evidence), in line with Ofcom's overarching objectives.

Engagement with complainants

Where Ofcom considers opening an investigation and / or opens an investigation following receipt of a complaint from an industry stakeholder, other enforcement agency[20] or whistle-blower, the Draft Enforcement Guidance allows for the possibility of extensive engagement between Ofcom and the complainant, including by meeting with the complainant, at various stages in the investigation process including:

- as part of the initial assessment process;[21]
- during the course of the investigation;[22]
- if Ofcom is considering changing the scope of an investigation (for example by providing the complainant the opportunity to comment on that decision);[23] and

[18] Annex 11, paragraph A4.2.

[19] Annex 11, paragraph A4.8.

[20] Meta has referred to other enforcement agencies here on the basis that they are mentioned as a possible complainant in Annex 11, paragraph A4.9. However, Meta's comments on engagement with complainants apply only to the extent that the complainant is not an enforcement agency.

[21] Annex 11, paragraphs A4.10 – A4.12.

[22] Annex 11, paragraph A5.24.

[23] Annex 11, paragraph A5.27.

- when Ofcom has drafted a provisional notice of contravention (the "**Provisional Notice**") - complainants may be provided with the opportunity to comment on a non-confidential copy of Provisional Notice and receive copies of, or access to, the underlying evidence relied upon in the Provisional Notice.[24]

Though Meta acknowledges that Ofcom may, in certain circumstances, need to engage with the complainant – for example at the outset of an investigation to allow it to obtain further information about the complaint the level of engagement being proposed by the Draft Enforcement Guidance goes beyond what would be typical in other regulatory contexts.

This is for several reasons:

- Complainants are highly unlikely to have detailed information about service providers' systems and processes and, instead, will almost certainly frame their complaints about specific examples of illegal or harmful content and include their personal views and perspectives on these. By committing in its guidance to regularly engaging with complainants throughout its investigations, Ofcom therefore risks signalling to prospective complainants and the public at large that it is willing to take into account complainants' subjective viewpoints as part of its otherwise objective and forensic investigation.
- Furthermore, committing to this level of engagement gives the impression that complainants will have some influence over the direction and decision-making in Ofcom's investigations. Notably, this is not an approach adopted by other "prosecuting authorities", likely for this very reason.
- The level of engagement with the complainant contemplated by the Draft Enforcement Guidance also risks affording the complainant special status compared to other members of the general public, who may be equally affected by any alleged deficiencies in the service providers' systems and processes but who, purely because they were not the party to complain, will not have the same opportunity as the complainant to engage with Ofcom's investigation.
- The proposed approach also creates challenges around the sharing of confidential information. As explained below, under the OSA, all information gathered by Ofcom from service providers cannot be further shared without that provider's consent.
- Investigations will often, for entirely understandable reasons, be non-linear: the scope of the investigation may change, interviews may need to be conducted multiple times, further information may need to be gathered etc. If Ofcom creates the expectation that it will provide regular updates on the investigation to complainants, then it will have to try and explain this process to the complainants, while abiding with the restrictions of information sharing, which is likely to be challenging and will almost certainly lead to dissatisfaction and misunderstanding on the part of the complainant.

Meta considers that, in line with the approach of the other UK regulators, following the submission of any complaint, the initial assessment, investigation and enforcement processes should be conducted by Ofcom alone, independent of the complainant. There should not be any regular updates on the status of the investigation to any third parties. This will facilitate the impartial, fair, efficient and timely conduct of the investigation. The communication to the complainant – and to the public at large – should only occur as per the provisions of the OSA: i.e. once a confirmation decision has been issued.

Publication of information

[24] Annex 11, paragraph A6.22.

The Draft Enforcement Guidance provides that Ofcom may publish details of any decision not to open an investigation and either: (i) resolve issues through means other than enforcement action (for example if Ofcom accepts assurances from a service provider); or (ii) take no further action. Where the service provider could be identified from the publication, Ofcom will usually inform that service provider and provide a copy of the intended text for information only.[25]

Ofcom further notes that, in the other regimes it regulates, Ofcom generally publishes information about investigations at the point it opens them and publishes updates at important milestones. Ofcom intends to adopt this approach in the online safety regime,[26] and does not intend to agree the text of website updates or media releases with the subject.[27]

The OSA does not require Ofcom to publish information regarding the opening of an investigation and / or updates on milestones and progress of the same. The only requirement imposed by the OSA on Ofcom to publish details of enforcement action applies when Ofcom has issued (and not withdrawn) a confirmation decision or a penalty notice.[28] Though Meta notes that the approach outlined in the Draft Enforcement Guidance is consistent with the approach Ofcom has taken in other regulatory regimes, for example the video-sharing platforms regime, it is out-of-step with the approach adopted by other UK regulators, for example by the FCA and PRA, which only typically publicly announces investigations in exceptional circumstances.[29]

Publishing information about the commencement of every investigation and regular updates about the same risks:

- creating expectations amongst the public, media and political figures as to the outcome of the investigation, especially given the risk that the public does not properly understand Ofcom's proposed approach to enforce against systemic failures rather than individual cases of harmful content;
- hindering the investigation process and putting pressure on Ofcom to resolve the case prematurely, irrespective of its merits;
- setting up Ofcom (and the service provider) for public dissatisfaction. From the outside, the public and press almost always think that investigations should be concluded far more quickly than they usually are. It is only once the specific circumstances and issues can be explained that it is possible to understand why investigations can take many months and often years. Given that Ofcom cannot provide this level of detail (as per the statutory restrictions on sharing information received under the OSA), providing what would be a generic "running commentary" on the investigation progress will almost certainly lead to dissatisfaction amongst the public and misunderstood and potentially misleading reporting in the press;
- negatively and unfairly impacting the subject of the investigation, including damaging the service provider's reputation. In the case of public companies like Meta, this could adversely impact their share price; and
- encouraging parallel litigation, even where no wrongdoing may eventually be found by Ofcom. This can be seen in other regulatory contexts, such as the parallel CMA

[25] Annex 11, paragraphs A4.24 and A4.29.

[26] Annex 11, paragraph A5.14.

[27] Annex 11, paragraph A5.19.

[28] OSA, s. 149.

[29] FCA Handbook, EG 6.1.1; The Prudential Regulation Authority's approach to enforcement: statutory statements of policy and procedure September 2021.

investigation and class action claim against Apple in relation to the App Store.[30] If this risk materialises in the online safety regime, service providers, Ofcom and the court will be faced with managing both regulatory investigations and parallel litigations, resulting in additional cost and complexity, even where Ofcom may eventually close the investigation without taking any further action.

In light of the risks outlined above, the approach proposed by Ofcom is particularly disproportionate in circumstances where Ofcom may eventually: (i) resolve issues through means other than enforcement action (for example if Ofcom accepts assurances from a service provider); or (ii) take no further action. Meta therefore suggests that Ofcom should reconsider its approach to publication of information and only publish any information at the stage at which the decision to issue a confirmation decision and / or penalty notice is issued. This reflects the requirements of the OSA.

Meta notes that the Draft Enforcement Guidance provides that there may be exceptional cases where Ofcom does not consider it appropriate to publicise.[31] Meta suggests that this position should be inverted: and Ofcom should only publicise investigation milestones where there are exceptional circumstances that justify it. This would align with the approach of other regulatory regimes and prevent the risks outlined above from materialising.

Provision of confidential information gathered during the investigation

The Draft Enforcement Guidance states that service providers who provide confidential information,[32] to Ofcom during an investigation should clearly identify it as such and explain the reasons why the information is considered confidential.[33]

In accordance with s. 383 of the Communication Act 2003, as recently amended by s. 115 of the OSA, "*information with respect to a particular business which has been obtained in exercise of a power conferred by*" the OSA shall not be disclosed without consent of the person carrying on that business. Therefore, under statute, information provided by a business pursuant to Ofcom's exercising its powers under the OSA is automatically confidential: it does not require a business to label it as such or to justify why it is confidential.

Therefore, Meta suggests that Ofcom's guidance should reflect the statutory position that all information provided by service providers pursuant to the exercise of Ofcom's powers under the OSA is deemed confidential, unless the service provider expressly confirms otherwise.

Settlement

Settlement discounts

Meta is supportive of Ofcom's indication that settlement discounts will be available as a matter of principle.[34] Meta notes that Ofcom will determine the appropriate settlement discount on a

[30] The CMA commenced its investigation into Apple on 3 March 2021 and an application for a collective proceedings order against Apple in relation to the same underlying facts was made in the Competition Appeal Tribunal on 11 May 2021, just over two months later. This CMA investigation is still ongoing in parallel to the class action.

[31] Annex 11, paragraph A5.21.

[32] Defined as "*commercially sensitive information or information relating to the private affairs of an individual*" at Annex 11, paragraph A5.47.

[33] Annex 11, paragraph A5.47.

[34] Annex 11, paragraphs A8.8 and A8.9.

case-by-case basis and the discount available will depend on the point at which settlement is reached. In particular:

- up to a maximum of 30%, where a successful settlement process is commenced before a Provisional Notice is issued;
- up to a maximum of 20%, where a successful settlement process is commenced after the Provisional Notice is issued, but prior to Ofcom receiving written representations; or
- up to a maximum of 10% where a successful settlement process is commenced after the Provisional Notice is issued and after Ofcom receives written representations.[35]

Meta considers that the maximum settlement discount of 30% should be available for all settlements agreed prior to Ofcom issuing a confirmation decision under s. 132 of the OSA. This is akin to the settlement approach adopted by the FCA, pursuant to which the investigation subject can secure a 30% discount if an agreement is concluded during a 28-day stage 1 settlement process – in this case the equivalent would be for the service provider to agree the terms of a confirmation decision with Ofcom within a specified time frame after Ofcom shares the draft with the service provider. Such an approach would encourage settlement and facilitate an effective and efficient resolution of Ofcom's enforcement process.

Decision making

The Draft Enforcement Guidance provides that the decision maker for settlement will typically be the person responsible for overseeing the investigation (i.e. the case supervisor).[36] It further states that the decision maker will oversee the settlement process and be responsible for taking the final decision on the case in the event the settlement process is successful.

Meta considers that the decision maker for settlement should be independent to the case team. It is human nature that, having conducted the investigation, the case supervisor and their team will have formed relatively set views about the issue in question and the sanction that they feel is appropriate. They are therefore inevitably less likely to adopt an open and independent mindset when it comes to discussing settlement than a party who has not been involved in investigating the underlying conduct.

This challenge has been recognised, and indeed resolved, in other regulatory regimes. For the FCA, the final settlement decision has to be taken jointly by two members of the FCA's senior management,[37] at least one of whom is not from the Enforcement and Financial Crime Division and both "*will not have been directly involved in establishing the evidence on which the decision is based*".[38]

For example, Meta is aware that in the context of resolving FCA investigations, the presence of independent settlement decision makers is often key to bridging the inevitable differences of views on the facts and the appropriate outcome between the subject of the investigation and the investigating case team. Indeed, the fact that the vast majority of FCA and PRA investigations are resolved through settlement is testament to the effectiveness of this measure.

[35] Annex 11, paragraph A8.9.

[36] Annex 11, paragraph A8.12.

[37] DEPP 5.1.1G(3).

[38] DEPP 5.1.1G(4).

Meta considers that no matter how fairly Ofcom's decision-making process may operate in practice, any perception of unfairness will undermine service providers' and the public's confidence in the same. This risks leading to fewer settlements and may also increase the frequency of challenge to Ofcom's enforcement decisions, decreasing efficiency and increasing the cost of the enforcement process.

For the above reasons, Meta suggests that the decision-making process in the Draft Enforcement Guidance be revised to adopt a model of independent decision makers akin to that used by the FCA. To the extent Ofcom does not adopt Meta's proposed approach, Meta would welcome further clarity on the basis on which Ofcom considers it appropriate not to adopt this approach, given the separation of decision making is widely considered to be good regulatory practice.

Admissions made on a statement of facts

Ofcom states that when the settlement process is commenced prior to a Provisional Notice, it is unlikely to be appropriate to pursue settlement if the subject of the investigation is not prepared to agree to a settlement based on the statement of facts prepared by Ofcom.[39]

This approach differs from that adopted in the financial services context and introduces a rigidity that is unlikely to be conducive to achieving settlement. In our advisors' experience, typically a main point of negotiation in settlement discussions with a regulator is ensuring that the systems, processes or conduct in question is described accurately and fairly in the summary to the satisfaction of the regulator and the provider. If the subject of an investigation was instead required to accept the regulators' first draft of this, many settlements simply would not occur. This is clearly not in the public interest, the interests of Ofcom or any regulated provider.

In light of the benefits offered by settlement, namely the swifter resolution of issues which will enable Ofcom to get its message to the market more quickly, efficiency for the public purse and reduce the resource impact on Ofcom, Meta considers that a core part of the settlement process should be Ofcom and the service provider agreeing the appropriate form of a statement of facts. A service provider's reluctance to accept Ofcom's initial proposed statement of facts should not preclude settlement altogether.

In the event Ofcom does not agree with Meta's suggestion, Meta would welcome further clarity on why Ofcom considers that it is unlikely to be appropriate to pursue settlement in those circumstances, particularly given the significant reduction in the penalty discount available to the service provider following the issue of the Provisional Notice (which will likely reduce a service provider's willingness to settle).

Without prejudice negotiations

The Draft Enforcement Guidance states that settlement is not akin to "*without prejudice*" negotiations for the purposes of seeking to resolve litigation.[40] Any additional documentary evidence provided during the settlement process would be placed on the case file and could be considered by Ofcom for the purposes of its final decision, even if the settlement process is unsuccessful. In addition, Ofcom may follow up any new issues of regulatory concern which come to light during the settlement process.

[39] Annex 11, paragraph A8.17.

[40] Annex 11, paragraph A8.33.

The Draft Enforcement Guidance is unclear on why Ofcom considers it appropriate to depart from the standard principle of settlement which is that such discussions are held on a without prejudice basis. In the regulatory context specifically, the without prejudice status of settlement discussions is necessary to prevent any admissions made by a service provider during the settlement process in an attempt to reach a genuine resolution of the matter subsequently being used against the service provider, for example in an appeal to the Upper Tribunal. The idea behind this is that settlement is only likely to occur if both parties know that any admissions and concessions they make in trying to reach a settlement won't later prejudice them in subsequent proceedings. By stating that settlement negotiations will instead be held on an open basis, Ofcom's proposed approach is likely to deter service providers from open discussions, making admissions or concessions and therefore make settlement unlikely, in turn increasing the time and costs required to conduct the investigation. For the proposed settlement process to be a viable option for service providers, Meta considers it is very important that settlement discussions are conducted on a without prejudice basis and any admissions or concessions made by a service provider during those discussions cannot be shared with: ● the final decision-maker for a confirmation decision, nominated as per A6.7; and ● the Upper Tribunal or any further courts that may consider the enforcement action.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Please see our response to Question 53 (i).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Annex 13: Impact Assessments

Question 54: **Response by Meta**
i) Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response: We have no comment on this.
ii) If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response: We have no comment on this.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.