HM Government

Online Harms White Paper - Initial consultation response

February 2020

This publication is available at
https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

Contents

Joint ministerial foreword

This is an exciting and unprecedented age of digital opportunity, and this government is committed to unleashing the full power of this country's first-class technology and boosting our standing in the world. Digital advances will undoubtedly drive our economy and enrich our society, but to fully harness the internet's advantages, we must confront the online threats and harms it can propagate, and protect those who are vulnerable to them.

That's why we want to make the UK the safest place in the world to be online and the best place to start and grow a digital business. We will make sure the benefits of technology are spread more widely and shared more fairly. Our approach is guided by the need to promote fair and efficient markets where the benefits of technology are shared widely across communities; ensure the safety and security of those online; and maintain a thriving democracy and society, where pluralism and freedom of expression are protected.

By getting it right, we will drive growth and stimulate innovation and new ideas, whilst giving confidence and certainty to innovators and building trust amongst consumers. As we leave the EU, we have an incredible opportunity to lead the world in regulatory innovation.
As the internet continues to grow and transform our lives it is essential that we get the balance right between a thriving, open and vibrant virtual world, and one in which users are protected from harm.

The scale, severity and complexity of online child sexual exploitation and abuse is a concern for government, law enforcement and companies, with 16.8 million referrals of child sexual

abuse material by US technology companies to the National Center for Missing and Exploited Children in 2019. In the UK, law enforcement is making 500 arrests and safeguarding 700 children a month as a result of these referrals and other sources.

Terrorist propaganda and vile online child sexual abuse destroy lives and tear families and communities apart. We cannot allow these harmful behaviours and content to undermine the significant benefits that the digital revolution can offer.

Two thirds of adults in the UK are concerned about content online, and close to half say that they have seen hateful content in the past year. Online abuse can have a severe impact on people's lives and is often targeted at the most vulnerable in our society. Cyberbullying has been shown to have psychological and emotional impact. In a large survey of young people who had been cyberbullied, 37% had developed depression and 26% had suicidal thoughts. These figures are higher than corresponding statistics for 'offline' bullying, indicating the increased potential for harm.
This update shares some of the findings from the Online Harms White Paper consultation, as we work to ensure the digital revolution works for families, communities and businesses. We are grateful to everybody who responded to the consultation on our proposals to eradicate these corrosive and abhorrent harms. There were some clear themes amongst the responses which we will pay close attention to as we move towards the legislation announced in the Queen's Speech.

Firstly, freedom of expression, and the role of a free press, is vital to a healthy democracy. We will ensure that there are safeguards in the legislation, so companies and the new regulator have a clear responsibility to protect users' rights online, including freedom of expression and the need to maintain a vibrant and diverse public square.

We are also introducing greater transparency about content removal, with the opportunity for users to appeal. We will not prevent adults from accessing or posting legal content, nor require companies to remove specific pieces of legal content. The new regulatory framework will instead require companies, where relevant, to explicitly state what content and behaviour is acceptable on their sites and then for platforms to enforce this consistently.
Secondly, respondents emphasised the need for clarity and certainty for businesses, and proportionate regulation. Analysis so far suggests that fewer than 5% of UK businesses will be in scope of this regulatory framework. The 'duty of care' will only apply to companies that facilitate the sharing of user generated content, for example through comments, forums or video sharing. Just because a business has a social media presence, does not mean it will be in scope of the regulation. Business to business services, which provide virtual infrastructure to businesses for storing and sharing content, will not have requirements placed on them.

Thirdly, many respondents reinforced the importance of higher levels of protection for children, which will be reflected in the policy we develop through this consultation. The proposals assume a higher level of protection for children than for the typical adult user, including, where appropriate, measures to prevent children from accessing age-inappropriate or harmful content. This approach will achieve a more consistent and

comprehensive approach to harmful content across different sites and go further than the Digital Economy Act's focus on online pornography on commercial adult sites.

On the question of who will be taking on the role of the regulator, having listened to feedback from this consultation, we are minded to appoint Ofcom. This would allow us to build on Ofcom's expertise, avoid fragmentation of the regulatory landscape and enable quick progress on this important issue.
We are a pro-technology government and we are keen to continue to work with industry to drive forward the digital agenda. We are continuing to work at pace to ensure the right regulatory regime and legislation is in place. The ICO has recently published its Age Appropriate Design Code, and more detailed proposals on online harms regulation will be released in the spring alongside interim voluntary codes on tackling online terrorist and child sexual exploitation and abuse content and activity.

In the meantime, we will continue our efforts to unlock the huge opportunities presented by digital technologies whilst minimising the risks.

To ensure that we keep momentum on a comprehensive package of measures we will be publishing and undertaking further work to address online harms, such as:

- government media literacy strategy
- The Law Commission's consultation on abusive and offensive online communications
- a review into the market for technology designed to improve online safety, where the UK is a leading innovator
- developing our understanding and evidence base of online harms and approaches to tackling them. This is why we have supported cross-government research to understand how platforms can recognise their child users through age assurance

We are confident that this publication, and the other plans we are driving forward, will help us to achieve our objectives; making Britain the safest place to be online and the best digital economy in the world.

The Rt Hon Baroness Morgan of Cotes

Secretary of State, Department for Digital, Culture, Media & Sport

The Rt Hon Priti Patel MP

Secretary of State, Home Office

Executive summary

1.The Online Harms White Paper set out the intention to improve protections for users online through the introduction of a new duty of care on companies and an independent regulator responsible for overseeing this framework. The White Paper proposed that this regulation follow a proportionate and risk-based approach, and that the duty of care be designed to ensure that all companies have appropriate systems and processes in place to react to concerns over harmful content and improve the safety of their users - from effective complaint mechanisms to transparent decision-making over actions taken in response to reports of harm.

2.The consultation ran from 8 April 2019 to 1 July 2019. It received over 2,400 responses ranging from companies in the technology industry including large tech giants and small and medium sized enterprises, academics, think tanks, children's charities, rights groups, publishers, governmental organisations and individuals. In parallel to the consultation process, we have undertaken extensive engagement over the last 12 months with representatives from industry, civil society and others. This engagement is reflected in the response.

3.This initial government response provides an overview of the consultation responses and wider engagement on the proposals in the White Paper. It includes an in-depth breakdown of the responses to each of the 18 consultation questions asked in relation to the White Paper proposals, and an overview of the feedback in response to our engagement with stakeholders. This document forms an iterative part of the policy development process. We are committed to taking a deliberative and open approach to ensure that we get the detail of this complex and novel policy right. While it does not provide a detailed update on all policy proposals, it does give an indication of our direction of travel in a number of key areas raised as overarching concern across some responses.

4.In particular, while the risk-based and proportionate approach proposed by the White Paper was positively received by those we consulted with, written responses and our engagement highlighted questions over a number of areas, including freedom of expression and the businesses in scope of the duty of care. Having carefully considered the information gained during this process, we have made a number of developments to our policies. These are clarified in the 'Our Response' section below.

5.This consultation has been a critical part of the development of this policy and we are grateful to those who took part. This feedback is being factored into the development of this policy, and we will continue to engage with users, industry and civil society as we continue to refine our policies ahead of publication of the full policy response. We believe that an agile and proportionate approach to regulation, developed in collaboration with stakeholders, will strengthen a free and open internet by providing a framework that builds public trust, while encouraging innovation and providing confidence to investors.

Our response

Freedom of expression

1.The consultation responses indicated that some respondents were concerned that the proposals could impact freedom of expression online. We recognise the critical importance of freedom of expression, both as a fundamental right in itself and as an essential enabler of the full range of other human rights protected by UK and international law. As a result, the overarching principle of the regulation of online harms is to protect users' rights online, including the rights of children and freedom of expression. Safeguards for freedom of expression have been built in throughout the framework. Rather than requiring the removal of specific pieces of legal content, regulation will focus on the wider systems and processes that platforms have in place to deal with online harms, while maintaining a proportionate and risk-based approach.

2.To ensure protections for freedom of expression, regulation will establish differentiated expectations on companies for illegal content and activity, versus conduct that is not illegal but has the potential to cause harm. Regulation will therefore not force companies to remove specific pieces of legal content. The new regulatory framework will instead require companies, where relevant, to explicitly state what content and behaviour they deem to be acceptable on their sites and enforce this consistently and transparently. All companies in scope will need to ensure a higher level of protection for children, and take reasonable steps to protect them from inappropriate or harmful content.

3.Services in scope of the regulation will need to ensure that illegal content is removed expeditiously and that the risk of it appearing is minimised by effective systems. Reflecting the threat to national security and the physical safety of children, companies will be required to take particularly robust action to tackle terrorist content and online child sexual exploitation and abuse.

4.Recognising concerns about freedom of expression, the regulator will not investigate or adjudicate on individual complaints. Companies will be able to decide what type of legal content or behaviour is acceptable on their services, but must take reasonable steps to protect children from harm. They will need to set this out in clear and accessible terms and conditions and enforce these effectively, consistently and transparently. The proposed approach will improve transparency for users about which content is and is not acceptable on different platforms, and will enhance users' ability to challenge removal of content where this occurs.

5.Companies will be required to have effective and proportionate user redress mechanisms which will enable users to report harmful content and to challenge content takedown where necessary. This will give users clearer, more effective and more accessible avenues to question content takedown, which is an important safeguard for the right to freedom of expression. These processes will need to be transparent, in line with terms and conditions, and consistently applied.

Ensuring clarity for businesses

6.We recognise the need for businesses to have certainty, and will ensure that guidance is provided to help businesses understand potential risks arising from different types of service, and the actions that businesses
ould need to take to comply with the duty of care as a result. We will ensure that the regulator consults with relevant stakeholders to ensure the guidance is clear and practicable.

Businesses in scope

7.The legislation will only apply to companies that provide services or use functionality on their websites which facilitate the sharing of user generated content or user interactions, for example through comments, forums or video sharing. Our assessment is that only a very small proportion of UK businesses (estimated to account to less than 5%) fit within that definition. To ensure clarity, guidance will be provided by the regulator to help businesses understand whether or not the services they provide or functionality contained on their website would fall into the scope of the regulation.

8.Just because a business has a social media page that does not bring it in scope of regulation. Equally, a business would not be brought in scope purely by providing referral or discount codes on its website to be shared with other potential customers on social media. It would be the social media platform hosting the content that is in scope, not the business using its services to advertise or promote their company. To be in scope, a business would have to operate its own website with the functionality to enable sharing of user- generated content, or user interactions. We will introduce this legislation proportionately, minimising the regulatory burden on small businesses. Most small businesses where there is a lower risk of harm occurring will not have to make disproportionately burdensome changes to their service to be compliant with the proposed regulation.

9.Regulation must be proportionate and based on evidence of risk of harm and what can feasibly be expected of companies. We anticipate that the regulator would assess the business impacts of any new requirements it introduces. Final policy positions on proportionality will, therefore, align with the evidence of risk of harm and impact to business. Business-to-business services have very limited opportunities to prevent harm occurring to individuals and as such will be out of scope of regulation.

Identity of the regulator

11.We are minded to make Ofcom the new regulator, in preference to giving this function to a new body or to another existing organisation. This preference is based on its organisational experience, robustness, and experience of delivering challenging, high-profile remits across a range of sectors. Ofcom is a well-established and experienced regulator, recently assuming high profile roles such as regulation of the BBC. Ofcom’s focus on the communications sector means it already has relationships with many of the major players in

the online arena, and its spectrum licensing duties mean that it is practised at dealing with large numbers of small businesses.

12.We judge that such a role is best served by an existing regulator with a proven track record of experience, expertise and credibility. We think that the best fit for this role is Ofcom, both in terms of policy alignment and organisational experience - for instance, in their existing work, Ofcom already takes the risk-based approach that we expect the online harms regulator will need to employ.

Transparency

13.Effective transparency reporting will help ensure that content removal is well-founded and freedom of expression is protected. In particular, increasing transparency around the reasons behind, and prevalence of, content removal may address concerns about some companies' existing processes for removing content. Companies' existing processes have in some cases been criticised for being opaque and hard to challenge.

14.The government is committed to ensuring that conversations about this policy are ongoing, and that stakeholders are being engaged to mitigate concerns. In order to achieve this, we have recently established a multi-stakeholder Transparency Working Group chaired by the Minister for Digital and Broadband which includes representation from all sides of the debate, including from industry and civil society. This group will feed into the government's transparency report, which was announced in the Online Harms White Paper and which we intend to publish in the coming months.

15.Some stakeholders expressed concerns about a potential 'one size fits all' approach to transparency, and the material costs for companies associated with reporting. In line with the overarching principles of the regulatory framework, the reporting requirements that a company may have to comply with will also vary in proportion with the type of service that is being provided, and the risk factors involved. To maintain a proportionate and risk-based approach, the regulator will apply minimum thresholds in determining the level of detail that an in-scope business would need to provide in its transparency reporting, or whether it would need to produce reports at all.

Ensuring that the regulator acts proportionately

16.The consideration of freedom of expression is at the heart of our policy development, and we will ensure that appropriate safeguards are included throughout the legislation. By taking action to address harmful online behaviours, we are confident that our approach will support more people to enjoy their right to freedom of expression and participate in online discussions.

17.At the same time, we also remain confident that proposals will not place an undue burden on business. Companies will be expected to take reasonable and proportionate steps to protect users. This will vary according to the organisation's associated risk, first and

foremost, size and the resources available to it, as well as by the risk associated with the service provided. To ensure clarity about how the duty of care could be fulfilled, we will ensure there is sufficient clarity in the regulation and codes of practice about the applicable expectations on business, including where businesses are exempt from certain requirements due to their size or risk.

18.This will help companies to comply with the legislation, and to feel confident that they have done so appropriately.

Enforcement

19.We recognise the importance of the regulator having a range of enforcement powers that it uses in a fair, proportionate and transparent way. It is equally essential that company executives are sufficiently incentivised to take online safety seriously and that the regulator can take action when they fail to do so. We are considering the responses to the consultation on senior management liability and business disruption measures and will set out our final policy position in the Spring.

Protection of children

20.Under our proposals we expect companies to use a proportionate range of tools including age assurance, and age verification technologies to prevent children from accessing age-inappropriate content and to protect them from other harms. This would achieve our objective of protecting children from online pornography, and would also fulfil the aims of the Digital Economy Act.

Next steps

1.Online Harms is a key legislative priority for this government, and we have a comprehensive programme of work planned to ensure that we keep momentum until legislation is introduced as soon as parliamentary time
allows. As mentioned above, this is an iterative step as we consider how best to approach this complex and important issue. We will continue to engage closely with industry and civil society as we finalise the remaining policy. While preparation of legislation continues, and in addition to the full response to be published in the spring, we are developing other wider measures in order to ensure progress now on online safety. These will include:

Interim codes of practice

2.The government expects companies to take action now to tackle harmful content or activity on their services. For those harms where there is a risk to national security or to the safety of children, the government is working with law enforcement and other relevant bodies to produce interim codes of practice.

3.The interim codes of practice will provide guidance to companies on how to tackle online terrorist and Child Sexual Exploitation and Abuse (CSEA) content and activity. The codes will be voluntary but are intended to bridge the gap until the regulator becomes operational, given the seriousness of these harms. We are continuing to engage with key stakeholders in the development of the codes to ensure that they are effective. We will publish these interim codes of practice in the coming months.

Government transparency report

4.The Online Harms White Paper committed the government to producing its first annual transparency report. We intend to publish this report in the next few months. The report will be informed by discussions at a multi- stakeholder Transparency Working Group chaired by the Minister for Digital and Broadband.

Non-legislative measures

5.The White Paper made clear that all users should have the tools and resources available to manage their own online safety, and that of others in their care. It committed the government to developing a media literacy strategy and we announced in the government's response to the Cairncross Review that the strategy would be published in summer 2020. The media literacy strategy will ensure a coordinated and strategic approach to online media literacy education and awareness for children, young people and adults. It will aim to support citizens as users in managing their privacy settings and their online footprint, thinking critically about the things they come across online (disinformation, catfishing etc), and how the terms of service and moderating processes can be used to report harmful content. We will publish this in the summer of 2020.

6.We are keen to continue to work in partnership with tech companies and wider stakeholders to refine our approach, and to work on collaborative solutions, especially looking at how we can use technology to tackle these issues. Industries such as the safety tech sector are central to the government's aim to promote innovation and develop a flourishing tech industry that also delivers technological solutions to meet regulatory requirements. To that end, we can also announce the upcoming publication of a full report into the safety technology ecosystem, which will identify opportunities for increasing competition and quality within the sector.

Wider regulation and governance of the digital landscape

7.As well as delivering on our commitments set out in the Online Harms White Paper, the government is undertaking an ambitious programme of wider work on how we govern digital technologies to unlock the huge opportunities presented by digital technologies whilst minimising the risks. Work on electoral integrity and related online transparency issues is being taken forward as part of the Defending Democracy programme together with the Cabinet Office.

8.We want the wider institutional landscape for digital technologies to be future-proof and fit for the digital age. As a result, over the coming months we will engage experts, regulators, industry, civil society and the general public to ensure our overarching regulatory regime for digital technologies is fully coherent, efficient, and effective.

Chapter one: Detailed findings from the consultation

1.The next sections cover:

- Chapter One: Methodology of the written consultation and engagement with stakeholders across industry, civil society, international partners and user groups
- Chapter Two: Responses on the regulatory framework (ie scope, user redress, industry transparency, enforcement options and appeals)
- Chapter Three: Responses on the proposals for the independent regulator, regulatory accountability and funding models
- Chapter Four: Responses to the non-legislative measures: the opportunities and challenges around technological innovation, safety by design, child online safety and education and awareness

Methodology - public consultation

2.Following the White Paper's publication, we undertook a formal 12-week public written consultation, complemented by an extensive programme of stakeholder engagement. The written consultation took place between April and July 2019, and included 18 questions on aspects of the government's plans for regulation and tackling online harms. In total, we gathered 2,439 responses from across academia, civil society, industry and the general public. The face-to-face stakeholder engagement enabled a constructive dialogue with key stakeholders, and those groups that may have been underrepresented in the written consultation.

Written consultation

3.We gathered written consultation responses via an online portal, email and post, both from organisations and from members of the public. Not all respondents engaged with every question - and indeed the response ate dropped throughout the questions. Of the 18 questions, 6 were closed questions with predefined response options on the online portal, allowing us to provide statistics for the responses to these questions for those who responded via the portal. These statistics, therefore, represent 63% of all responses (69% of all individuals and 32% of all organisations), and do not represent the major organisational respondents.

4.The remainder of the questions invited free text qualitative responses and each response was individually analysed. The response summaries below include the key themes and issues highlighted across all responses, but do not include statistics due to the nature of these questions.

5.A notable number of individual respondents to the written consultation disagreed with the overall proposals set out in the White Paper. Those respondents often seemed not to engage with the substance of questions on the specific proposals, but instead reiterated a general disagreement with the overall approach. This was most notable in those questions

on regulatory advice, proportionality, the identity and funding of the regulator, innovation and safety by design, which seemed to attract a relatively large amount of confusion in responses. For these respondents, it was therefore difficult to delineate between an objection to the overall regime and an objection to the specific proposal within the question.

Profile of respondents

6.In total we received 1,531 online responses and 908 responses via email. 84% of these responses were from individuals and 16% from organisations (including tech sector, civil society, charities etc).

7.We collected demographic information for just over 90% of individuals who responded via the online portal, covering 58% of all responses:

- Age: The largest proportions of responses were from those aged 45-54 (21%) and 55-64 (17%), followed by those aged 35-44 (16%) and 25-34 (15%). Respondents aged 18-24 and over 65 each made up 13% of the sample while 5% were under 18
- Gender: Almost three quarters (72%) of respondents identified as male, with around a quarter (24%) female and 4% identified as “other”
- Ethnicity: A little under two thirds (60%) of respondents identified as “White British/English/Welsh/Scottish/Northern Irish”. Followed by 11% “White: Any other background”, 3% “asian”, 2% “mixed/multiple ethnic groups” and “Black/African/Caribbean background” respectively. Fewer than 1% identified as “Arab”, 13% selected “other” and 9% preferred not to say
- Disability: Just over one in ten (11%) consider themselves as disabled under the Equality Act 2010, 75% do not and 14% preferred not to say.

8.As these demographics indicate, this sample, as with all written consultation samples, may not be representative of public opinion as some key groups are over- or under-represented.

9.A number of ‘campaigns’ were organised in response to the consultation from three sources: Samaritans, Open Rights Group, and Hacked Off. These responses were either identical or very similar and were submitted through central coordination. These responses were analysed and included in the same way as all other responses.

Engagement

10.Over the 12 week period we held 100 meetings, which supported the written consultation. This engagement enabled detailed conversations with a wide range of stakeholders and ensured we heard the views of important groups. Our engagement reflected the range of organisations that may be in scope of the online harms regulatory framework, including tech organisations, the games industry and retail. We also engaged with academia, regulators and civil society. Furthermore, we consulted the devolved administrations and discussed the policy in international multi-stakeholder fora and with international partners.

11.We recognise that some abuse or content which targets users based on actual or perceived protected characteristics under the Equality Act 2010 means that some people face disproportionately negative experiences online. In line with this, during the consultation period we conducted workshops with groups representing users with various protected characteristics. This included engaging with a range of user groups representing those who are likely to be disportionately affected by online harms, such as the LGBTQ+ community; survivors of abuse and violence; disabled users; mental health organisations; religious groups; children, parents and child safety organisations. This engagement ensured groups were able to feed back expert knowledge on specific issues faced by the users they represent.

12.Engagement included a series of thematic workshops to consult on the core White Paper policies. These workshops focused on: the scope of regulation; transparency; enforcement powers; technology as a solution; safety by design; the regulator; user complaints; media literacy and education. Other meetings included 17 ministerial engagements, 'deepdive' sessions with major technology companies, and roundtable meetings with industry associations. We also engaged stakeholders on specific, key issues raised following the White Paper's release, including the regulation of the press and freedom of expression, and the approach to the interim codes of practice on terrorist content and child sexual exploitation and abuse.

Summary of response findings:

13.The key themes from responses to the consultation and our engagement were:

- The White Paper stated, on the activities and organisations in scope, that the regulatory framework will apply to online providers that supply services or tools which allow, enable or facilitate users to share or discover user-generated content or interact with each other online. Respondents welcomed the targeted, proportionate and risk based approach that the regulator is expected to take. Responses also highlighted the need to ensure that proposals remain flexible and able to respond as technology develops in the future. Companies and stakeholders, however, asked for more detail on the breadth of both services and harms in scope. Responses focused on ensuring that freedom of expression is protected.

- The White Paper made clear that under the new duty of care, companies will need to ensure they have user redress mechanisms in place. This would mean that companies need to have effective, accessible complaints and reporting mechanisms for users to raise concerns about specific pieces of harmful content or activity and seek redress. The White Paper also highlighted a role for designated bodies to make 'super complaints' to the regulator to defend the needs of users. Respondents welcomed this, and highlighted the importance of ensuring that companies have effective reporting mechanisms for harmful content, accessible to all users. Organisations showed stronger support for the proposals for super- complaints than individuals did. Broadly, respondents requested more guidance on how a super-

complaints function could work, and how it could take into account accountability and transparency mechanisms.

- On transparency, the White Paper set out that companies in scope will be required to issue annual transparency reports. Respondents to the consultation as well as the stakeholders who were engaged highlighted the importance of transparency, both in terms of reporting processes and moderation practices. They see this as being central in holding companies accountable for enforcement of their own standards. Industry respondents suggested that transparency requirements should be proportionate – noting that a 'one size fits all' approach was unlikely to be effective and could be costly to implement for smaller companies.

- The White Paper set out that the regulator will have an escalating range of powers to take enforcement action against companies that fail to fulfil their duty of care - including notices and warnings, fines, business disruption measures, but also senior manager liability, and Internet Service Provider (ISP) blocking in the most egregious cases. Respondents to the consultation as well as the stakeholders who were engaged recognised the role for a tiered enforcement structure, ensuring that enforcement powers are used fairly and proportionately. Civil society groups overall expressed support for firm enforcement actions in cases of non-compliance. Industry and rights groups expressed some concerns about the impact of some of the measures on the UK's attractiveness to the tech sector and on freedom of expression. They sought further clarity on the intervention and escalation structure, including the grounds for enforcement. They want the regulator to support compliance with the regime in the first instance.

- The White Paper proposed that companies have nominated representatives in the UK, to assist the regulator in taking enforcement action against companies based overseas. Respondents acknowledged that this system would support the effectiveness of the proposed legislation, however concerns were raised about the potential impact on smaller businesses.

- The White Paper set out that the regulator will offer regulatory advice to companies on reasonable expectations for compliance, based on both the severity and scale of the harm, the age of their users and the size of the company and resources available to it. Respondents welcomed this. The main suggestions provided were on opportunities for the regulator to provide clarity on any specific standards and thresholds, alongside guidelines and expert advice on how organisations could comply.

- The White Paper acknowledged that online harms can materialise via private communications services, and committed to setting out a differentiated framework for harm over private communications. Responses across stakeholders recognised the balance between taking appropriate action to address the serious harms, such as child grooming, that can be initiated and escalate from private forums and ensuring appropriate protections for users' privacy. Most companies and organisations agreed that expectations of private services to tackle harm should be greater, firstly where

content and activity is illegal, and secondly where children are involved. Most respondents opposed the inclusion of private communication services in scope of regulation. However, some responses - both from individuals and organisations acknowledged that abuse, harassment and some of the most serious illegal activity occur in private spaces, like closed community forums and chat rooms. These responses expressed support for the principle that platforms should be responsible for their users' safety in private channels.

- The White Paper set out that there must be an appeals mechanism for companies and others to challenge against a decision by the regulator when appropriate. Responses showed broad support for a mechanism allowing appeals against enforcement action by the regulator. Companies suggested that appeals mechanisms should be quick and affordable, focussed on the merits of the action taken and that administrative processes should be as streamlined as possible.

- The White Paper stated that proportionality would be central to enforcement decisions by the regulator. Respondents welcomed the suggestion that the compliance systems could be designed similarly to current models in, for example, the finance sector. Specifically, they expressed support for options allowing companies to self-assess whether their services are in scope, and enabling members of the public to raise concerns with the regulator where a company is not complying.

- The White Paper did not express a specific preference for the identity of the regulator. Most of the stakeholders we engaged with had no particular preference. Responses were supportive of a new body or of extending the duties of an existing regulator. Some feared that the latter option could prove overwhelming for an existing body and thus instead voiced support for a transitional or temporary body.

- The White Paper set out that the regulator will be cost-neutral, and that for funding it would recoup costs via charges or a levy on companies in scope. Companies who responded to the consultation viewed the application of a charge with concern, citing worries around potential double or disproportionate costs to certain services and exemption for others.

- The White Paper proposed a duty on the regulator to lay an annual report and accounts before Parliament and provide Parliament with information as and when requested for accountability. All groups generally expressed support for Parliament to have a defined oversight role over the regulator in order to hold it to account, maintain independence from government and build public trust and hold industry confidence.

- The White Paper committed to developing a framework on safety by design and innovation, to make it easier for start-ups and small businesses to embed safety in their products. Stakeholders expressed broad agreement and recognition that safety is improved when organisations build in user-safety at the design and development stage of their online services. They also emphasised that machine learning solutions

require extensive data and were supportive of the ‘regulatory sandbox’ model (i.e. allowing businesses to test innovations in a controlled environment).

- The White Paper committed to make the UK the safest place to be online, having key regard for child online safety. Respondents welcomed this, and one of the key themes of our engagement was parents’ concerns about the safety of their children online. In particular, although parents felt that they know their children best and are therefore usually the best placed to tailor standard advice for them, they also agreed on the need for more advice and education on how to be online safely.

- The White Paper recognised that users want to be empowered to manage their safety online, and that the regulator should consider education and awareness to support this. Throughout our engagement, digital education and awareness were key recurring themes. Many felt that the regulator could have an important role in creating a framework for evaluating the impact of existing education and awareness activity in their space. Others recognised that there could be a role for the regulator or for government in supporting the most vulnerable children and disseminating alerts about emerging online threats for young people.

Chapter two: Regulatory framework

1.The Online Harms White Paper set out the intention to bring in a new duty of care on companies towards their users, with an independent regulator to oversee this framework. The approach will be proportionate and risk-based with the duty of care designed to ensure companies have appropriate systems and processes in place to improve the safety of their users.

2.The White Paper stated that the regulatory framework will apply to online providers that supply services or tools which allow, enable or facilitate users to share or discover user-generated content, or to interact with each other online. The government will set the parameters for the regulatory framework, including specifying which services are in scope of the regime, the requirements put upon them, user redress mechanisms and the enforcement powers of the regulator.

3.The consultation responses indicated that some respondents were concerned that the proposals could impact freedom of expression online. We recognise the critical importance of freedom of expression, and an overarching principle of the regulation of online harms is to protect users' rights online, including the rights of children and freedom of expression. In fact, the new regulatory framework will not require the removal of specific pieces of legal content. Instead, it will focus on the wider systems and processes that platforms have in place to deal with online harms, while maintaining a proportionate and risk-based approach.

4.To ensure protections for freedom of expression, regulation will establish differentiated expectations on companies for illegal content and activity, versus conduct that may not be illegal but has the potential to cause harm, such as online bullying, intimidation in public life, or self-harm and suicide imagery.
5.In-scope services will need to ensure that illegal content is removed expeditiously and that the risk of it appearing is minimised by effective systems. Reflecting the threat to national security and the physical safety of children, companies will be required to take particularly robust action to tackle terrorist content and online child sexual exploitation and abuse.

6.Companies will be able to decide what type of legal content or behaviour is acceptable on their services. They will need to set this out in clear and accessible terms and conditions and enforce these effectively, consistently and transparently.

7.We do not expect there to be a code of practice for each category of harmful content. We recognise that this would pose an unreasonable regulatory burden on in-scope services. However, we will publish interim codes of practice in the coming months to provide guidance for companies on how to tackle online terrorist and CSEA content and activity. The codes will be voluntary but are intended to bridge the gap and incentivise companies to take early action prior to the regulator becoming operational, thus continuing to promote behaviour change from industry on the most serious online harms. We are continuing to engage with key stakeholders in the development of the codes to ensure that they are effective.

8.We will expect the regulator to set expectations around imagery that may not be visibly illegal, but is linked to child sexual exploitation and abuse, for example, a series of images, some of which were taken prior to or after the act of abuse itself. We will consider further how to address this issue through the duty of care.

9.The legislation will only apply to companies that provide services which facilitate the sharing of user generated content or user interactions, for example through comments, forums or video sharing. Only a very small proportion of UK businesses (estimated to account for less than 5%) fit within that definition. To ensure clarity, guidance would be provided to help businesses understand whether or not the services they provide would fall into the scope of the regulation.

10.To be in scope, a business's own website would need to provide functionalities that enable sharing of user generated content or user interactions. We will introduce this legislation proportionately. We will pay particular attention to minimising the regulatory burden on small businesses and where there is a lower risk of harm occurring.

11.We have listened to and taken into account feedback from industry stakeholders. It is clear that business- to-business services have very limited opportunities to prevent harm occurring to individuals and as such remain out of scope of the Duty of Care.

12.We are continuing the work on the final details of the organisations in scope, to ensure proportionality and effective implementation of our proposals. We will produce an impact assessment to accompany legislation which will take into account burdens to businesses.

Activities and organisations in scope

Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

Engagement

13.Throughout our engagement, organisations expressed support for the targeted, proportionate, and risk- based approach for the regulator. Many parties expressed a need for clarity as the proposals develop around the kind of organisation and platforms that would be in scope.

14.The tech industry, while broadly supportive, emphasised the importance of providing clear definitions of the companies and harms in scope, in particular addressing what is meant by 'user generated content'. A number of organisations suggested that business to business (B2B) services should not be in scope, as their view was that there was a lower risk that the harms covered in the White Paper would develop on such platforms. Press freedom organisations and media actors also expressed the view that journalistic content should not

be in scope, to protect freedom of expression and in accordance with established conventions of press regulation.

15.Civil society organisations representing disadvantaged groups demonstrated strong support for the proposals and emphasised the importance of including any provider of a platform or service made available to users in the UK within the scope of the regulation. Women's groups , LGBT+, disability, and religious groups cited larger social media companies most frequently as the platforms of greatest concern, but were also concerned about smaller platforms, chat rooms, and anonymous apps, which they believe can easily be infiltrated for harm. A number of organisations suggested that economic harms (for instance, fraud) should be in scope. While the White Paper was clear that the list of harms provided was not intended to be exhaustive or definitive, a number of organisations suggested specific harms, for example misogyny. Many civil society organisations also raised concerns about the inclusion of harms which are harder to identify, such as disinformation, citing concerns of the impact this could have on freedom of expression.

Written consultation

16.Just over half of respondents to the written consultation answered this question. Responses which expressed support for the proposed platforms and activities in scope called on the government to increase education and public awareness of online harms. Responses also stressed the need to ensure that the proposals remain flexible and able to change as technology develops in the future, and that they maintain a special focus on young people and children.

17.Many respondents expressed concerns around the potential for the scope of the regulator to be too broad or for it to have an adverse impact on freedom of expression. Many of these respondents, therefore, called for further clarification of services and harms in scope. Some respondents also raised concerns that the proposals
ould have disproportionate impacts on specific organisations or, on the other hand, that they may not go far enough.

A systems based approach to online safety

The White Paper outlined a systems based approach:

- The duty of care is designed to ensure companies have appropriate systems and processes in place to improve the safety of their users.
- The focus on robust processes and systems rather than individual pieces of content means it will remain effective even as new harms emerge. It will also ensure that service providers develop, clearly communicate and enforce their own thresholds for harmful but legal content.
- Of course, companies will be required to take particularly robust action to tackle terrorist content and online Child Sexual Exploitation and Abuse. The new regulatory framework will not remove companies' existing duty to remove illegal content.

18.When broken down, the responses from organisations and members of the public differed in regard to the main perceived issues. For instance, concerns for freedom of expression were significantly more prevalent amongst individual respondents than amongst organisations. Instead, organisations reported a higher concern around the overreach of scope and a need for further clarity.

19.In general, organisations were more supportive of regulation when compared to public respondents. The tech sector and civil society groups expressed a level of support for the activities listed in scope, with many agreeing that focus should be on risk of harm, and that the regulator should take a proportionate approach to the companies in scope according to their risk profile.

20.At the same time, almost all industry respondents asked for greater clarity about definitions of harms, and highlighted the subjectivity inherent in identifying many of the harms, especially those which are legal. The majority of respondents objected to the latter being in scope.

21.Regarding harms in scope, several respondents stated that the 23 harms listed in the White Paper were overly broad and argued that too many codes of practice would cause confusion, duplication, and potentially, an over-reliance on removal of content by risk-averse companies. We do not expect there to be a code of practice for each category of harmful content, however, as set out above we intend to publish interim codes of practice on how to tackle online terrorist and Child Sexual Exploitation and Abuse (CSEA) content and activity in the coming months.

22.Specific groups echoed many of the general points raised in the written consultation, as well as suggesting specific services for inclusion in scope. For example, counter-extremism and religious groups noted the need for clarity to ensure that harms can properly be protected against and to minimise risks to constraining free expression. A common perspective among children's charities was that gaming should be in scope.

23.Across responses and engagement, there was broad support for the proposed targeted, proportionate and risk-based approach that the regulator is expected to take. Responses also highlighted the need to ensure that proposals remain flexible and able to respond as technology develops in the future. However, companies and stakeholders wanted more detail on the breadth of both services and harms in scope. There was also a consistent focus on ensuring that freedom of expression was protected. Respondents welcomed the focus on protecting vulnerable users, including young people and children, and a number of respondents also suggested that further work should be done to increase education and public awareness of online harms.

User redress

24.The White Paper recognised that companies' claims of having a strong track record on online safety are often at odds with users' reported experiences. The White Paper made clear that, under the new duty of care, government expects companies to ensure they have

effective, accessible complaints and reporting mechanisms for users to raise concerns about specific pieces of harmful content or activity and seek redress, or to raise wider concerns that the company has breached its duty of care. The White Paper also highlighted a role for designated bodies to make 'super complaints' to the regulator to defend the needs of users.

25.The regulator will have oversight of these processes, including through transparency information about the volume and outcome of complaints, and the power to require improvements where necessary. The regulator will be focused on oversight of complaints processes, it will not make decisions on individual pieces of content.

26.Recognising concerns about freedom of expression, while the regulator will not investigate or adjudicate on individual complaints, companies will be required to have effective and proportionate user redress mechanisms which will enable users to report harmful content and to challenge content takedown where necessary. This will give users clearer, more effective and more accessible avenues to question content takedown, which is an important safeguard for the right to freedom of expression. These processes will need to be transparent, in line with terms and conditions, and consistently applied.

Should designated bodies be able to bring super complaints to the regulator in specific and clearly evidenced circumstances? If your answer is yes, in what circumstances should this happen?

What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

Engagement

27.While the written consultation did not directly ask about internal company processes, many organisations shared their views in written responses and in supporting stakeholder engagement. They overwhelmingly agreed that companies should have effective and accessible mechanisms for reporting harmful content and felt that current processes often fell short. They agreed that this process should start with reports directly to the platform. Some respondents, including disability and children's advocates, noted the importance of making these mechanisms accessible and prominent for all users, as they are often not easy to find on websites. Some also noted the importance of companies providing explanations to users whose content is removed, in order to protect rights and to help all users understand what is acceptable on different platforms. Some respondents also argued for a more standardised approach to reporting complaints to enable comparison and analysis
.
28.A number of organisations highlighted concerns about a potential risk that the regulator would become the arbiter of what is considered harmful and the potential impact of this on freedom of expression.

29.A recurrent theme in organisational responses was that more effective complaints and reporting processes must also be accompanied by education and awareness-raising by companies and other stakeholders, including on people's rights and responsibilities and the avenues available to them to raise concerns. Nevertheless, as the section summarising responses to the question of how users should be educated shows, there was no consensus on which body or bodies should be responsible for educating users.

30.We stated that we do not envisage a role for the regulator itself in determining disputes between individuals and companies. Several organisations agreed with this, noting that it would not be feasible for the egulator to look into individual complaints and that it could risk users' rights to freedom of expression. Other espondents instead suggested that the regulator should have powers to look at specific cases, for example those which are particularly high-profile or serious.

Written consultation

31.The White Paper written consultation included a specific question on whether legislative provision should be made for designated bodies to bring 'super-complaints' to the regulator for consideration, in specific and clearly evidenced circumstances. 88% of respondents online answered this question, of whom almost a third (32%) agreed with the proposal and almost half (49%) disagreed. The remainder (19%) said they did not know.

Figure 1: Should designated bodies be able to bring super complaints to the regulator in specific and clearly evidenced circumstances? Note: Online portal respondents only.

32.When considering organisational responses only, the proportion of respondents who agreed with the proposal rises to almost two-thirds (63%). The majority of stakeholders with whom we engaged also supported super-complaints. Many noted that super-complaints could prove particularly useful for tackling issues regarding legal harms, which cannot be addressed through law enforcement agency routes. Groups representing religious users felt that super-complaints could provide an effective means to address online discrimination and

abuse. Disability and children's advocacy groups, as well as some academics, were especially supportive, noting that super-complaints would allow for people who might not otherwise raise concerns or report issues to be heard and to have their concerns alerted to the regulator.

33.Several organisational respondents sought further clarity on how a super-complaints function would work in practice, and others (including regulators with super-complaint functions) noted that they are not normally intended to deliver direct redress to individuals. Women's charities expressed support, but noted that other mechanisms may be necessary, for example in the case of low-level continuous harassment, which causes distress through its repetitiveness rather than its content. Some respondents also noted that a super-complaints function would only be effective if it was transparent and backed up by accountability mechanisms.

34.For those answering 'yes', we asked a further question on the circumstances under which super complaints should be admissible. Among organisational respondents, there was a high level of agreement that super-complaints should be permitted when there has been a large number of complaints or where there is evidence of clear abuses of company policy or standards. However , there was little consensus on what the criteria would look like in practice. There were relatively few individual responses to this question, as individuals responding online were only shown the question if they had responded 'yes' to part one. Of those individuals who did respond, there was little consensus, although in general individuals were more supportive than organisations of super-complaints regarding specific pieces of content.

35.We also consulted on other measures for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care. Less than two fifths of respondents answered this question, and while the majority of responses expressed general disagreement with the proposals, a significant number expressed support and proposed options for users to raise concerns.

36.Many responses, particularly from organisations, argued for an independent review mechanism, such as an ombudsman, although no-one gave further detail on how this could work and some organisations raised concerns about the feasibility and desirability of an ombudsman. Other proposals included the possibility for automatic suspensions of reported posts on request by regulator or individuals.

37.While many individual respondents raised concerns about freedom of expression and how the envisaged user redress framework will be implemented in practice, there was a general consensus amongst organisations about the need for effective and accessible mechanisms for users to seek redress, and in favour of the measures we proposed.

Protecting users' rights online

The White Paper stressed that users should receive timely, clear and transparent responses to their complaints of harmful content and committed to protecting their rights.

- **Companies covered by the regulator will be required to have an effective, proportionate, easy-to-access complaints process, allowing users to raise concerns about harmful content or activity, or that the company has breached its duty of care.**
- **The regulator will set minimum standards for these processes, so that users will know how they can raise a complaint, how long it will take a company to investigate, and what response they can expect.**
- **We do not envisage a role for the regulator itself in determining disputes between individuals and companies, but where users raise concerns with the regulator, it will be able to use this information as part of its consideration of whether a company may have breached duty of care.**

38.The importance of ensuring that companies should have effective reporting mechanisms for harmful content, accessible to all users, was highlighted here. There was stronger support for the proposals for super- complaints from organisations responding than from individuals, with organisations highlighting that super- complaints could provide particularly useful for addressing legal-but-harmful content prevalent on some platforms. Broadly, respondents requested more support on how a super-complaints function could work, and how it could take into account accountability and transparency mechanisms. A number of respondents suggested a role for an independent review mechanism.

Transparency

39.As set out in the White Paper, the government has committed to giving the regulator the power to require annual transparency reports from companies in scope. These reports would, for example, outline the prevalence of harmful content on their platforms, and what measures are being taken to address these.

40.The regulator would publish these reports online to support users and parents in making informed decisions about internet use. The regulator would also have powers to require additional information from companies to inform its oversight or enforcement activity, and to establish requirements to disclose information.

41.Effective transparency reporting will help ensure that content removal is well-founded and freedom of expression is protected. In particular, increasing transparency around the reasons behind, and prevalence of, content removal may address concerns about some companies' existing processes for removing content. Companies' existing processes have in some cases been criticised for being opaque and hard to challenge.

42.In addition, as part of the transparency reporting framework, the regulator will encourage companies to share anonymised information with independent researchers, and ensure companies make relevant information available.

43.The government is committed to ensuring that conversations about this policy are ongoing, and that stakeholders are being engaged to mitigate concerns. In order to achieve this, we have recently established a multi-stakeholder Transparency Working Group chaired by the Minister for Digital and Broadband, which includes representation from all sides of the debate, including civil society members as well as industry. This group will feed into the government's transparency report, which was announced in the Online Harms White Paper and which we intend to publish in the coming months.

44.Some stakeholders expressed concerns about a potential 'one size fits all' approach to transparency, and the material costs for companies associated with reporting. The regulatory framework is designed to be proportionate, and so will set out minimum thresholds that a company would need to meet before reporting requirements would apply. In line with the overarching principles of the regulatory framework, the reporting requirements that a company may have to comply with will also vary in proportion with the type of service that is being provided, and the risk factors involved.

The government has committed to Annual Transparency Reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

Engagement

45.Transparency has been a key theme discussed with a range of organisations and user groups. A wide variety of stakeholders, including rights groups and tech companies, supported such measures and agreed that increased transparency is needed. Children's charities, LGBT+ organisations and religious groups especially welcomed the framework's focus on transparency - both in terms of reporting processes and moderation practices for the purpose of holding companies accountable to their own standards. Freedom of expression groups were similarly supportive of greater transparency and accountability but were keen to emphasise that transparency reporting should promote users' rights and should contain information about how companies uphold users' right to freedom of expression online.

46.The importance of proportionality in relation to the transparency requirements emerged as a key point. Furthermore, a number of companies noted that, given the variation between companies, a 'one size fits all approach' was unlikely to be effective.

Written consultation

47.The written consultation asked people whether, beyond the measures set out in the White Paper, the government should do more to build a culture of transparency, trust and accountability across industry and, if so, what? 90% of online respondents answered this closed question. Of these, there was little difference between those who agreed the government should do more and those who disagreed (41% and 39% respectively). Almost a fifth (19%) said they didn't know.

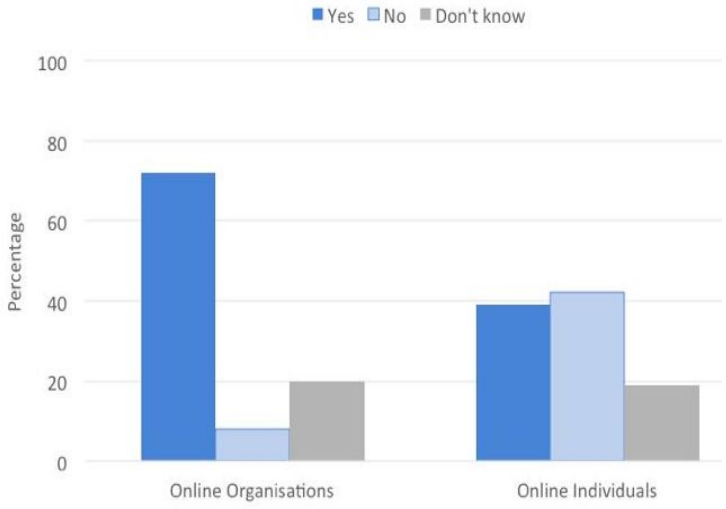

Figure 2: The government has committed to Annual Transparency Reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry? Note: Online portal respondents only.

48.When broken down, the responses from organisations and members of the public differ, with 72% of organisations agreeing that the government should do more, compared to only 39% of individuals.

49.Those who agreed that the government should do more provided answers for how and what measures could go beyond the White Paper proposals to increase transparency. A large proportion of responses suggested this could be done through requiring increased clarity and detail of reporting. Many responses also suggested that engagement with international partners would help to promote a culture of transparency and trust.

50.In particular, amongst organisations, civil society groups were considerably more supportive of the proposals advanced in the White Paper around transparency, which they saw as a crucial mechanism to increase companies' accountability and foster positive relationships with the regulator. While the technology sector was also overall broadly supportive of transparency, there was less consensus about the format the eporting should take. Some small and medium sized enterprises (SMEs) highlighted resource and capability

challenges associated with collecting or reporting certain types of information. Other respondents, including dating sites and retailers, echoed this concern, stating that transparency reporting might be overly onerous on them should it require significant re-engineering of their given product or service if it had not been designed to gather certain types of data. Generally, respondents expressed support for flexibility over rigid guidelines, although, at the same time, some did acknowledge the benefit of having structure and direction from the regulator.

51.Many responses also explicitly mentioned that reporting should be qualitative, not just quantitative, avoiding a one size fits all approach, and that the data reported should be clear and meaningful. Respondents also asked that transparency reports be written in plain English and made accessible to the public.

52.Responses from both organisations and individuals contained specific proposals for how to increase transparency. These proposals included requiring social media companies to show how safety features are being improved in line with the regulator's recommendations. Other suggestions included: increased transparency from social media platforms on content moderation decisions, involving the public in formulating online harms policy and encouraging social media companies to promote their own transparency reports to their users.

53.Responses also suggested specific focal points and metrics for the transparency report, such as an independent review of AI/algorithms, an attention to 'addiction by design,' a specific separate focus on child safety, advertising, and finally expert medical advice.
54.Additionally, although not directly relevant to the question, many responses took the opportunity to suggest an increase in government transparency and that any future regulator should also be transparent.

55.Many of those who disagreed that the government should do more asserted that government should not be involved or should be less involved. Other responses attested that it was not possible to hold the companies in scope to account.

56.Overall, responses to this question varied, expressing suggestions for what government should do to increase transparency, trust and accountability across industry, as well as some respondents expressing concerns with an increasing government role.

Enforcement

57.The regulator will have a range of enforcement powers to take action against companies that fail to fulfil their duty of care. This will drive rapid remedial action, and ensure that non-compliance faces serious consequences. The enforcement powers referenced are the power to issue warnings, notices and substantial fines. The White Paper also included proposals for business disruption measures - including potential for business disruption, Internet Service provider (ISP) blocking, senior management liability.

Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

Engagement

58.Throughout our engagement, industry representatives ranging from larger tech firms to start-up companies expressed a measure of support for the tiered enforcement approach set out in the White Paper. At the same time, they asked for further clarity on what would be considered appropriate points for intervention and escalation, as well as what limits could be considered reasonable for sanctions in order for these not to represent an unacceptable business risk. Internet service provider (ISP) blocking represented the main area of concern across discussions. Industry stated in principle support in some cases (e.g. when websites are set up for solely unlawful purposes), but argued that it would need to be mandated only as a last resort following due process and underpinned by the legal framework.

59.Senior manager liability emerged as an area of concern. Discussions with industry highlighted the risk of potential negative impacts on the attractiveness of the UK tech sector. Further concerns emerged that this approach may unduly penalise individuals for content often originating from other third-parties who would not be adversely affected by the sanctions, unless the regime proposed is able to account for these. With regard to further powers, industry representatives felt that the regulator should fulfill a supervisory function and look to support compliance in the first instance.

60.Civil society groups overall expressed support for firm enforcement actions, in cases of non-compliance. Nevertheless, rights organisations expressed concerns about risks to freedom of expression and the potential impact of censorship associated with enforcement powers.

Written consultation

61.The written consultation specifically asked whether the regulator should be empowered to:

- disrupt business activities
- undertake ISP blocking
- implement a regime for senior management liability

62.We also asked if any further powers should be available to the regulator.

63.This question did not receive a high response rate. Across all categories, the majority of respondents highlighted concerns that excessive enforcement could have a detrimental effect on both business and personal freedoms - and risk that measures could incentivise companies to over-block user-generated content to avoid penalties.

64.Analysis of the responses of organisations and individuals showed a large difference in levels of support - with a significantly larger portion of concerns coming from the individual respondents, while organisations generally supported the proposals. This result is not surprising given the apprehension amongst many individual respondents about how the proposals would impact usability and personal freedoms. The creative industries, sport sector, local government, law enforcement organisations and children's charities particularly expressed broad support for the majority of enforcement mechanisms listed in the White Paper.

65.Respondents who supported the proposals took the view that the regulator should have robust enforcement powers that are used fairly and proportionately.

66.Respondents expressing support for the business disruption proposals highlighted the importance of the need to ensure these powers are used proportionately and should be an escalation from demonstrable non- compliance and prior warnings being issued. This view was also expressed for senior management liability. Many who welcomed it as a measure to hold individuals to account felt it should only be used after demonstrable non-compliance and the failure of previous measures. For ISP blocking the common view was that it be used as a last resort. A small number of respondents suggested additional powers, including further enforcement measures against companies such as temporary content takedowns, and sanctions for failing to duly protect freedom of expression.

67.Organisations raised other points of criticism. Rights groups expressed concerns that the proposed enforcement approach may be disproportionately punitive, and the regulator would need to demonstrate it had met the proportionality test for freedom of expression under human rights law. This was a particular concern for ISP blocking.

68.Although many industry members noted their opposition to ISP blocking in general, they acknowledged that there may be circumstances in which the exercise of such powers would be appropriate. Practically, industry requested clear guidance and an agreed process for notifying operators when websites are required to be blocked (or reinstated), and clarification on the anticipated volume of websites that would be in scope.

69.From a technical perspective, Internet Service Providers (ISPs) also noted the importance of developing the future regulation with reference to wider technical developments such as encryption, which might undermine the effectiveness of website blocking. Industry requested a transition period to adjust to or implement the new regulations without the threat of severe sanctions. Larger tech companies highlighted the implementation challenges they may have due to the size and complexity of their systems.

70.In summary, while civil society groups overall expressed support for firm enforcement actions, the proposals remain contentious for industry, freedom of expression groups, and members of the public. For the implementation of the proposed measures, respondents expressed a preference for the regulator to begin its operations by supervising companies

and supporting compliance through advice, and that any further enforcement measures should be used proportionately and following a clear process.

Nominated Representative

71.Noting the particularly serious nature of some of the harms in scope and the global nature of many online services, the White Paper proposed that the regulator should have the power to ensure that action can be taken against companies without a legal presence in the UK. It sets out the possibility of a requirement for companies to nominate a UK or EEA-based representative for these purposes, similar to the concept in the EU's General Data Protection Regulation (GDPR).

Should the regulator have the power to require a company based outside the UK or EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

Engagement

72.Throughout our engagement with industry, concerns of impracticality and challenges of implementation merged as a key theme, with SMEs arguing that this could be excessively burdensome for them. Some proposed other ideas, such as the establishment of an endorsement system for companies demonstrating best practice.

Written consultation

73.Less than half of online respondents answered this question (48%), of which almost two thirds (62%) responded"no", followed by "yes" (27%) and "don't know" (11%). Respondents to the written consultation generally disagreed that the regulator should have the power to require a company based outside the UK or EEA to appoint a nominated UK or EEA representative.

Figure 3: Should the regulator have the power to require a company based outside the UK or EEA to appoint a nominated representative in the UK or EEA in certain circumstances? Note: Online portal respondents only.

74.When broken down by organisations and members of the public, the responses are contrasting, with the majority of organisations responding “yes” (63%) as opposed to less than a quarter of individuals (24%). Furthermore, the proportion of those that responded “don’t know” is larger amongst organisations than members of the public (25% and 10% respectively).

75.Across both groups, among those who agreed that the regulator should have the power to require a UK or EEA representative, many responses focused on this being necessary to support international consistency and cooperation. A large proportion of these responses highlighted a need for increased international dialogue, followed by consideration of issues such as online harms being too complex to be regulated in a single country.

76.Responses from organisations in particular often suggested that a representative would be necessary to enable UK legislation to be effective, aid the implementation of regulation and making it harder for companies to avoid complying.

77.Additionally, many responses suggested that the requirement to have a UK or EEA representative should only apply to organisations over a certain size or with a particular user base, echoing a theme that regulation should be proportionate.

78.Of the majority of all respondents who disagreed with the proposed requirement, the most common concern was around the potential negative impact on business. Some small business respondents explicitly expressed disagreement, feeling that this proposal would impose costs and demands that will negatively affect them.

79.Other concerns included: potential for a negative impact on users; a lack of effectiveness when the UK leaves the European Union; and concerns over how it could be practically enforced.

80.Overall, it is clear that the impacts of nominated representation on business costs and operations is a point of concern for industry, and SMEs in particular.

Regulatory advice

81.The White Paper set out how the regulator will take a proportionate approach, with reasonable expectations of companies dependent on both the severity and scale of the harm, the age of their users and the size of the company and resources available to it. The White Paper also set out the principles of better regulation, including a commitment for the regulator to help SMEs and start-ups to fulfill their obligations for compliance.

82.The written consultation asked how the regulator could provide advice and support to help businesses comply with the regulatory framework, acknowledging the potential for specific impacts to SMEs and start-ups.

What, if any, advice or support could the regulator provide to help businesses, particularly start-ups and SMEs, comply with the regulatory framework?

Engagement

83.Throughout our engagement with industry, the main ask was for the regulator to provide clarity over any specific standards as a basis for the new regulation.

Written consultation

84.Written responses provided a variety of suggestions for how the regulator could provide support to businesses. The most common response from both organisations and individuals was for guidelines and expert advice on how organisations need to comply, and for a need for effective engagement strategies.

85.Some responses made suggestions about the approach to regulation more generally, suggesting exemptions for start-ups and SMEs and a differentiated approach depending on the business type. Respondents also highlighted that engagement would need to be clear on how regulation interacts with international legal obligations. A number of responses, the majority from individuals, also expressed disagreement with the implicit assumption in the question that a regulator would be established, possibly further impacted by confusion in the role of regulators amongst some responses. A small proportion expressed that no advice or support should be provided to help businesses.

86.Organisations particularly emphasised the need for support and advice. SMEs and cloud service providers emphasised that they would like to see the regulator have an open door policy with business stakeholders and begin its operation offering advice through resources and “how-to” guides. Similarly, other respondents advanced suggestions that the regulator

offer, and have the power to charge for specific advice services to companies that request detailed advice on how they can comply with the regulations.

87.It is clear that organisations, particularly SMEs, want the regulator to provide guidance on how different services can fulfil the duty of care. Organisations also want to be able to contact the regulator for more tailored advice. They feel that the regulator should be able to provide advice at an early stage of its operation.

Private communications

88.The White Paper acknowledged both the importance of privacy online and the aim to protect UK users from harmful content or behaviour wherever it occurs online. It noted that criminals should not be able to exploit the online space to conduct illegal activity. The development of harmful activity online frequently involves a combination of activity taking place on both 'public' and 'private' communication channels. For example, people targeting children to commit serious online harms often make initial contact with a child on public social media platforms, before moving to private messaging services to continue the grooming process. The White Paper consulted on what criteria should be considered in developing a definition for 'private' communication services, noting the complexity of defining 'private' and 'public' in the online space.

89.Reflecting the importance of privacy, the White Paper committed to setting out a framework that will ensure a differentiated approach for private communication. The White Paper consulted on which channels or forums which could be considered private should be in scope of the regulatory framework. It asked what specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms.

In developing a definition for private communications, what criteria should be considered?

Which channels or forums that can be considered private should be in scope of the regulatory framework?

What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

Engagement

90.We engaged with experts from academia, industry, think tanks and wider civil society organisations on the questions of defining private communications, the scope of the regulatory framework in relation to private channels, and what requirements should be applied to private channels.

91.Throughout our engagement, organisations representing vulnerable groups expressed strong support for private communications falling in scope of the regulatory framework. Children's charities were particularly insistent that community forums, chat rooms and messaging apps all need to be in scope, providing evidence of how people targeting children to commit serious online harms use these services to groom and abuse children.

92.Industry representatives and some civil society groups expressed concern that to include private channels in scope might lead platforms to take steps that create unacceptable, negative impacts on users' privacy. Some civil society groups were more comfortable with online platforms empowering users to themselves report harmful activity on private channels, but expressed concern about more intrusive steps such as proactive moderation of private channels. Most companies and organisations agreed that the regulator's expectations of companies to tackle harms on private services should be greater where the content and activity is illegal and/or where children are involved.

Written consultation

93.Around a third of respondents answered question 6. Organisations were more likely to advance criteria for defining private communications than individual respondents. A common response was that user intent and purpose of the service should be taken into account when considering if a communication is private.

94.Several responses from organisations stated that one-to-one phone calls, messages, and video calls should not be included in scope and cautioned against using the number of users as the sole indicator for whether a communication is private. However, others state that identifying a maximum number of people beyond which a conversation is no longer considered private could be helpful.

95.In terms of which fora and services should be in scope, many organisations responded "none", and only a small proportion responded "all". In between these two, the other most common responses were based on suggestions for specific activities or platforms.

96.Those who answered "none" with regard to which private services should be in scope, when elaborating on their answer, argued that the presence of a blocking feature on a private service, enabling users to block content from other individuals, is sufficient for tackling harm. These respondents argued for the need to respect user privacy and also maintained that encrypted services be ruled out of scope.

97.Among those who expressed agreement with including private communications in scope, a large portion of responses from organisations mentioned specific activities and platforms to include, such as social media, dating, and gaming sites as well as services enabling private messaging, and video and photo sharing. These responses identified the significance of private communications as spaces where harms can be planned and carried out. Some responses also expressed concern about the migration of illegal activity - such as child grooming and the sharing of child abuse imagery - to encrypted spaces, arguing that encrypted services should be in scope.

98.Those respondents - both organisations and individuals - who responded ‘none’ to the question of which private services should be in scope also tended to answer ‘none’ to the question of which requirements should be applied to private services.

99.Those respondents who agreed that some private communication services should be in scope provided a range of answers to the question of which requirements should be applied to private services. These included suggestions of requirements which might limit the impact on users’ privacy. For example, responses suggested that platforms should offer reporting mechanisms allowing users to report abusive or offensive content sent to them privately - a process, which would not require companies to monitor private messages for harm.

100.In conclusion, overall respondents opposed the inclusion of private communication services in scope of regulation. However, there was acknowledgement in some responses - both from individuals and organisations - that abuse, and harassment and some of the most serious illegal activity occur in private spaces, like closed community forums and chat rooms. These responses expressed support for the principle that platforms should be responsible for their users’ safety in private channels.

Appeals

101.The White Paper acknowledged that companies and others must have confidence that the regulator is acting fairly and within its powers. As with other regulatory systems, companies will have the ability to seek a judicial review of the regulator’s decisions through the High Court. The White Paper also considered other avenues of appeal and asked whether there should be a further statutory mechanism for companies to appeal against a decision of the regulator. We gave the example of section 192-196 of the Communications Act 2003, through which there is the ability to appeal against an Ofcom decision via the Competition Appeal Tribunal.

In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

If your answer to question 14 is ‘yes’, in what circumstances should companies be able to use this statutory mechanism?

If your answer to question 14 is ‘yes’, should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

Engagement

1.During engagement, companies suggested that the appeals mechanism should be quick and affordable, and focused on the merits of the action taken. Companies mentioned blocking measures and app removal as areas where they would especially seek to be able to appeal regulator decisions. Companies also emphasised that for an appeals mechanism involving judicial scrutiny, an administrative process as seamless as possible would be needed to minimise bureaucratic burdens, and accelerate the process. SMEs expressed support for additional mechanisms other than Judicial Review due to concerns around the costs and overall accessibility of the latter.

Written consultation

Figure 4: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003? Note: Online portal respondents only.

103.Less than half of all online portal respondents (48%) answered this question. Of those who did over two thirds (71%) of respondents were in favour of such an additional statutory mechanism. 15% of respondents disagreed with such a mechanism and the remaining 14% said they did not know.

104.A relatively large proportion of respondents suggested specific circumstances where access to this appeal mechanism should be allowed. Respondents suggested that the mechanism be available in cases where decisions related to legal content that is not harmful, when it is claimed that the best effort was made to deal with an issue by the company, when the penalty applied is considered disproportionate, and if a company is adversely affected financially and operationally.

105.The second supplementary question (question 14b) asked whether the appeal should be decided on the basis of the principles that would be applied on an application for judicial review (i.e. whether the regulator in reaching its decision had acted lawfully and fairly) or on the merits of the specific case. An appeal on the merits of the case would involve a full reappraisal of both the facts and the applicable law relating to the regulator's original decision. The majority of responses were in favour of an appeal being decided on the merits of the case, but with minimal further commentary about the reasons for this preference.

106.Overall, responses were supportive of companies in scope of regulation being able to appeal decisions, offering a range of circumstances when companies may need to do this. Respondents did not provide further details about the advantages of a statutory appeals body in particular or how the duties of such a body could be discharged.

Chapter three: The regulator

1.The White Paper stated that the online harms regime will be overseen and enforced by an independent regulator. To inform the set up of this regulator, we asked a number of questions about the identity of the regulator, its funding model and accountability to Parliament.

2.The White Paper also explained that the government is carefully considering whether a broader restructuring of the regulatory landscape would reduce the risk of duplication and minimise burdens on business. Over the coming months we will engage experts, regulators, industry, civil society and the wider public to ensure our overarching regulatory regime for digital technologies is fully coherent, efficient, and effective. This is part of an ambitious programme of wider work to unlock the huge opportunities presented by digital technologies whilst minimising the risks.

Proportionality

What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

Engagement

3.In our engagement with industry, companies suggested a model whereby companies self assess whether their services are in scope, notifying the regulator if something goes wrong, and where members of the public would be able to raise concerns with the regulator where a company is not complying. Another suggestion was that, similar to the banking regulatory model, the regulator could build the scope through dialogue with industry, designating systemically important services on which higher responsibilities would be placed.

4.Freedom of expression groups suggested that further transparency requirements placed on the regulator, and the incorporation of a duty to respect freedom of expression within the codes of practice, would also serve to ensure proportionality.

5.The consideration of freedom of expression is at the heart of our policy development, and we will ensure that appropriate safeguards are included throughout the legislation. By reducing the prevalence of online abuse, we are confident that our approach will support more people to enjoy their right to freedom of expression and participate in online discussions.

6.At the same time, we also remain confident that proposals as set out here will not place an undue burden on business. Companies will be expected to take reasonable and proportionate steps to protect users. This will vary according to the organisation’s size and the resources available to it, as well as by the risk associated with the service provided. In

recognition of concerns raised about possible uncertainty about how the duty of care could be fulfilled, we will ensure that there is sufficient clarity in the regulation and codes of practice about the applicable expectations on business. This will help companies to comply with the legislation, and to feel confident that they have done so appropriately.

Written consultation

7.Around half of respondents answered this question. Those who responded positively suggested that the regulator take steps to:

- adopt an international approach
- prioritise vulnerable groups
- issue tight guidelines and code of practice
- clarify its scope
- follow a code of conduct
- work with other existing bodies from the tech sector (e.g. Ofcom)
- offer support and guidance
- receive expert advice/evidence and
- collaborate with industry players

8.Many industry respondents expressed approval for the targeted, proportionate, risk-based and systematic approach proposed in the White Paper.

9.Multiple responses proposed that the government carry out an economic impact assessment to determine the anticipated effect regulation will have upon businesses and the United Kingdom's economy. A number of individual respondents also expressed concerns, around the creation of the regulator and possible restrictions on freedom of expression.

10.In conclusion, responses identified that the government should take further steps to ensure the regulator will act in a targeted and proportionate manner. Respondents expected regulation to balance respect of freedom of expression standards, while applying reasonable requirements and providing appropriate support for business.

Proportionality

In the White Paper, we made it clear that the regulatory framework would be proportionate and that we would avoid imposing excessive burdens. For example, we said:

- **All companies will be required to take reasonable and proportionate action to tackle harms on their services, but we will minimise excessive burdens, particularly on small businesses and civil society organisations.**
- **The regulator's initial focus will be on those companies that pose the biggest and clearest risk of harm to users.**

- **The regulator will set clear expectations of what companies should do to tackle illegal activity and keep children safe online.**
- **The regulator will be required to assess the action of companies according to their size and resources, and the age of their users, as well as the risk and prevalence of harms on their service.**

Identity of regulator

11.The White Paper proposed to establish an independent regulator to implement, oversee and enforce the regulatory framework. The regulator will be equipped with the powers, resources and expertise it needs to effectively carry out its role. Ofcom was the only regulator referenced in the White Paper as a possible candidate.

12.We judge that such a role is best served by an existing regulator with a proven track record of experience, expertise and credibility. We are minded to appoint Ofcom as they present the best fit for this role, both in terms of policy alignment and organisational experience - for instance, in their existing work, Ofcom already take the risk-based approach that we have outlined above.

13.Our proposal also sits within a wider programme of work by the government to respond to the challenges and opportunities presented by digital technology, through carefully considering the wider institutional landscape to ensure an effective overall approach to digital regulation that avoids overlap and confusion.

Should an online harms regulator be: (i) a new public body, or (ii) an existing public body? If your answer to question 10 is (ii), which body or bodies should it be?

Engagement

14.In engaging with different groups we learned that most were neutral towards the identity of the regulator. Some stakeholders felt that the scope of work envisaged by the White Paper could overwhelm an existing regulator, but at the same time organisations recognised the inherent challenges of creating a new body and setting up operations to process an enormous volume of information, and voiced support for a transitional or temporary body.

15.Several organisations expressed a preference for Ofcom to be the new regulator, citing its regulatory expertise. Some civil society groups, particularly children’s charities, proposed the establishment of an interim body to reflect the urgency of the harms. Most of the big tech companies had no preference either way but stressed the point that the regulator should have the necessary capabilities, infrastructure, resources and expertise to function effectively.

16.During engagement, respondents emphasised the need for there to be consistency between existing and new regulatory regimes, with some suggesting a need for a coordinating body. In their view, the regulator should draw upon existing expertise across government and across current arrangements for self and co- regulation.

Written consultation

17.In the consultation we asked whether the proposed regulator should be a new public body or an existing public body. For those respondents who preferred an existing public body, we asked which body or bodies it should be.

18.The response rate via the online portal for this question was low at 38%, and of these a majority (62%) were in favour of a new public body.

19.There were a number of different reasons for respondents expressing a preference for a new body. Both organisations and individuals believed that there was a need for a new body with specific focus and expertise in tech and online safety. Other less frequent themes such as placing too much burden on an existing regulator or the need for a regulator to be independent from government were also identified in the written responses.

20.Over a third of those responding (38%) favoured an existing body; citing a variety of reasons. The experience of existing organisations and their understanding of the sector were the two most significant and recurring advantages highlighted. Respondents also believed it would be cheaper to set up the regulator within an existing body.

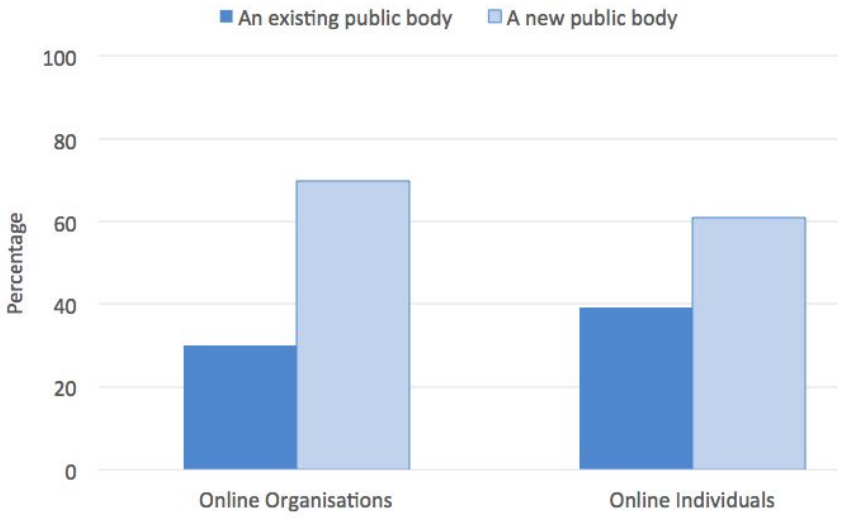

Figure 5: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body? If your answer to question 10 is (ii), which body or bodies should it be? Note: Online portal respondents only.

21.The sub-question (10a) asked, where respondents had expressed a preference for an existing body, which body it should be. This question received a variety of suggestions, with Ofcom receiving the greatest level of endorsement, particularly amongst organisations.

22.Other common suggestions for the regulator were the Information Commissioner's Office (ICO) and the police, and a very small proportion of respondents believed the courts should act as the regulator. Other respondents suggested a range of public and private bodies, such as the Advertising Standards Agency, or the UK Council for Internet Safety, but also government departments including DCMS, the Home Office and the Ministry of Justice.

23.Overall the response to this question demonstrated that the options on regulatory bodies for online harms come with different benefits and risks. Whilst a new body provides the opportunity for a dedicated focus and an innovative approach, it was suggested that it will be challenging to implement a new regulatory regime without the expertise, experience and organisational structure that an existing body brings.

24.We are minded to give Ofcom the role of the new regulator, in preference to giving this function to a new body or to another existing organisation. This preference is based on its organisational experience, robustness, and experience of delivering challenging, high-profile remits across a range of sectors. Ofcom is a well-established and experienced regulator, recently assuming high profile roles such as regulation of the BBC. Ofcom's focus on the communications sector means it already has relationships with many of the major players in the online arena, and its spectrum licensing duties mean that it is practised at dealing with large numbers of small businesses (both in terms of regulatory activity and fees collection). Further, Ofcom already takes a risk-based approach to investigations, similar to that envisaged for the Online Harms regulator. Ofcom would also remain subject to the Public Sector Equality Duty in its work on online harms, meaning that it must consider how its approach or decisions affect people with protected characteristics.

Funding

25.The White Paper makes clear that in order to recoup both the implementation costs and running costs of the regulator, the government is considering fees, charges or a levy on companies whose services are in scope. This could fund the full range of the regulator's activity. The government intends the new regulator to become cost neutral to the public sector.

A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

Engagement

26.During engagement, companies viewed the application of a charge/tax with concern. For some, there was risk that a regulatory charge or tax would amount to double taxation on the same businesses. Companies with only a small segment of their business activities within

the scope of the regulator requested clarity on how the regulator funding would be proportionate and affordable. Others contended that an unintended consequence of the charge/tax is that it could be diverting money away from businesses who may use it to address online harms. The collection of contributions from companies based overseas, particularly from smaller companies with a higher prevalence of online harms on their platforms compared to businesses in the UK, was expressed as a further concern.

27.Finally, some companies felt that a business's revenue/profit would not be an appropriate basis on which to determine funding contributions from industry, but instead the age profile of users and work currently being undertaken by a company to combat online harms should be taken into consideration. On the other hand, the companies acknowledged that the inclusion of any non-financial measures may lead to a charge or tax being subjective.

Written consultation

28.Around a third of respondents answered this question, suggesting a variety of considerations for funding contributions. The size and type of business was highlighted as being the main factor on which funding contributions should be determined. Beyond that, there was also support for licence fee/taxes on industry, from both organisations and individuals at broadly the same level.

29.There was some limited support from both individuals and organisations for the regulator to be funded by the government. There was also limited support for the regulator to be funded by fines against companies for breaking the law, and general funding from the private sector.

30.Many individual respondents expressed disagreement with the formation of the regulator, and, therefore, with the need for a funding mechanism and the proposal that industry should contribute.

31.In conclusion, respondents and stakeholders both agreed that whilst funding should primarily be from industry, the model should be proportionate and practical.

Accountability

32.The White Paper stated that the regulator will be an independent body and that it will be important to ensure that Parliament is able to scrutinise the regulator's work. We consulted on this and on what role Parliament should play in developing regulatory codes of practice.

33.As the White Paper notes, Parliament's role particularly "in relation to codes of practice and guidance issued…varies across different regulatory regimes, ranging from formal approval to no specific role". The starting point of accountability in the White Paper is a duty on the regulator to lay an annual report and accounts before Parliament and provide Parliament with information as and when requested.

What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

Engagement

34.During our engagement with stakeholders, all groups generally expressed support for Parliament to have a defined oversight role over the regulator in order to maintain independence from government and build public trust and hold industry confidence. Freedom of Expression groups advanced specific proposals calling for parliamentary oversight over codes of practice to protect fundamental freedoms. Several responses suggested establishing a dedicated body for reviewing codes to ensure consistency with civil liberties or establishing an independent Children's Digital Champion to inform and report on codes to Parliament. Some respondents suggested that the regulator should report targeted areas of concern in platform failures to allow Parliament to debate further evidence.

35.The most popular reason for giving Parliament a role, for both organisations and individuals, was the need to hold the regulator to account.

Written consultation

36.Broadly, responses showed strong support for parliamentary oversight, with various ideas on how this should be carried out. Many respondents called for the regulator to draft the codes of practice independently. Some responses proposed that codes of practice should be subject to public consultation and agreed by Parliament. A limited number of organisations and individual respondents believed that Parliament should have no role in scrutinising the role of the regulator.

37.Overall, respondents generally agreed that Parliament should have an important role in scrutinising the work of the regulator. Whilst some respondents advocated a more active role for parliament in developing codes of practice, others maintained that this would encroach upon the regulator's independence.

Codes of practice

The White Paper talked about the different codes of practice that the regulator will issue to outline the processes that companies need to adopt to help demonstrate that they have fulfilled their duty of care to their users.

- **The kind of processes the codes of practice will focus on are systems, procedures, technologies and investment, including in staffing, training and support of human moderators.**
- **As such, the codes of practice will contain guidance on, for example, what steps companies should take to ensure products and services are safe by design or deliver prompt action on harmful content or activity.**
- **Given the range of services in scope of the regulatory framework, some of the expectations below may not be applicable to every company.**

- **The primary responsibility for each company in scope is that they will be required to complete an assessment of the risk associated with its service(s) and take reasonable steps to guard against the risk of harm in order to fulfill its duty of care.**
- **We do not expect there to be a code of practice for each category of harmful content, however, we intend to publish interim codes of practice on how to tackle online terrorist and Child Sexual Exploitation and Abuse (CSEA) content and activity in the coming months.**

Chapter four: Non-legislative

1.Alongside the proposed regulatory framework, we are committed to implementing a number of non- legislative measures in order to ensure a holistic response to online harms. In order to inform these measures, the consultation asked questions about safety by design, children's online safety and media literacy.

Innovation and adoption of safety technologies

2.The White Paper set out the government's ambition to position the UK as a world leader in safety technology. It included commitments that the government and new regulator will work with leading industry bodies and other regulators to support innovation in and adoption of products and services that support user safety, and the growth of the UK's safety technology market. It proposed specific action to assess the online safety sector's capability and potential, and to explore how organisations can securely access training data to develop AI solutions while ensuring that AI use is safe and ethical.

What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

Engagement

1.During our engagement with industry, organisations emphasised that machine learning solutions required large amounts of training data. Several highlighted the opportunity for government or the regulator to enable the development of a system of common reference datasets, which third parties could use to safely and securely develop and test machine learning solutions. Organisations were supportive of the 'regulatory sandbox' model (ie. allowing businesses to test innovations in a controlled environment), and several respondents suggested that the data trust model could facilitate data sharing around online harms. Some organisations highlighted that machine learning still needs human assistance to identify context and nuance.

Written consultation

4.The written consultation asked respondents to identify the opportunities and barriers for innovation and adoption and to suggest how the government could work to address these. This question received a relatively low number of responses, particularly from individuals.

5.Where a response was given, a relatively large number of responses expressed disagreement with the overall proposals for regulation, with many focusing on concerns around freedom of expression. Many responses, in particular from individuals, did not engage with the different elements of the question, making it difficult in many cases to identify clear reasons for disagreement or concerns with the focus of the question.

6.Some respondents expressed concerns that regulation could stifle innovation if it was over-prescriptive, disproportionate or inflexible, or if a regulator did not have sufficient in-house technical capability. Conversely, several responses highlighted the positive role that regulators could play in supporting innovation, for example by increasing competition, preventing monopolies and addressing market failures.

7.In terms of opportunities, the most common one highlighted for innovation was the role that government could play through influence and advocacy, for example by supporting cross-sector initiatives to share technologies and ideas to tackle potential harms, and through using its convening power to help ensure closer collaboration and coordination across the value chain. In particular, organisations highlighted the positive role that groups such as the Technology Coalition and the Global Internet Forum to Counter Terrorism played in supporting the development and adoption of cross-sector solutions, such as hash-sharing databases for illegal content. A number of respondents felt that more action was needed to strengthen the evidence base used to inform and assess technical innovations - for example, through greater research into user behaviour online.

8.Some respondents to the written consultation focused on the role that government and the regulator could play in encouraging a competitive and world-leading market in online safety solutions, through which companies of all sizes could access a range of solutions to achieve safer outcomes for users. Several organisations felt that more could be done by government to articulate priorities for investment or innovation, or to identify the standards which safety technologies should adhere; to provide assistance in linking SMEs with larger organisations; and where appropriate to fund programmes of development support for startups and scaleups, for example through accelerators or incubator programmes.

9.In terms of the opportunities highlighted for adoption of safety technologies, many responses, particularly from organisations, highlighted the need to provide companies with high-quality information, training and guidance. Some responses focused on how regulation, government influence and public pressure also had the potential to drive adoption of safety technology.

10.Many of the barriers to both innovation and adoption were similar. Organisations were particularly concerned about the cost of innovation and adoption of safety technologies, and a potential lack of clear definitions of safety standards by a regulator. There was concern that smaller platforms' ability to innovate for safety might be restricted by regulation geared toward the capabilities and needs of larger platforms.

11.Overall, the consultation response suggested a number of ways in which the government or the regulator could support the innovation and adoption of safety technology. These were suggestions such as designing the regulatory framework to ensure that the goals of innovation and safety are intertwined, advocacy of the emerging safety tech sector, and enabling a data and AI infrastructure that supports innovation, competition and transparency. The main barrier highlighted for both innovation and adoption was the cost to businesses of such development.

Safety by Design

12.In the White Paper, the government committed to developing a safety by design framework to make it easier for start-ups and small businesses to embed safety during the design, development or updates of products and services.

What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

Engagement

13.Throughout our engagement with industry during the lead up to the Online Harms White Paper, stakeholders expressed broad agreement and recognition that standards of safety are improved when organisations build in user-safety at the design and development stage of their online services. They also recognised that a safety by design approach was needed for smaller companies in particular, and that the government should help them build capacity and technical expertise as they grow. Stakeholders also argued that assistance for designing safer services was specifically required in areas such as the needs of vulnerable users, age assurance, and more generally the different safety considerations applicable to children and adults.

Written consultation

14.This question had a relatively low number and wide variety of written responses, suggesting both drop off in the response rate and potential confusion amongst respondents due to the specificity of the question. This pattern of responses could also potentially indicate a lack of understanding amongst responders on what the principle of safety by design encompasses. This is compounded by the lack of specificity amongst the noticeable minority of, mostly individual, responses which expressed their disagreement with the overall proposals.

15.Of the responses which suggested areas for inclusion in the guidance, many seemed to focus on guidance in general and not specifically in areas that would enable organisations to build services that are safe by design. Educating users and new technologies were the most common areas highlighted as being those here organisations need guidance. Other responses also highlighted general compliance, data privacy, ethical guidance, encryption and content moderation.

16.Responses from organisations in particular highlighted child safety as a key area where organisations require guidance. This was followed by calls for overarching guidance on all areas, as well as age assurance. Responses from charities for girls and young women, and for other vulnerable groups, suggested that members of these groups should be actively involved and consulted in designing safe products.

17.During direct engagement over the consultation period, organisations also raised the need for broader organisational support and culture-changing efforts to help embed a safety by design approach. Organisations in particular felt that, while, specific guidance on high impact safety measures in many of the areas highlighted above are needed and effective, interventions further “upstream” in the design process would also be an impactful way to deliver a safety by design approach - and for this, they argued, government guidance is needed. They also recognised that support on safety by design needs to address all levels within an organisation to be effective at driving change.

18.Overall, it is clear that there is a strong feeling amongst organisations that greater guidance to enable a safety by design approach is needed. The breadth of the responses and the general lack of specificity on what type of intervention would be helpful also suggests that greater education is required on the function and objective of ‘safety by design’. Work is taking place to develop the key emerging themes, including guidance on specific high impact safety measures and supporting safety interventions upstream in the design process. For example, work is already underway with the VoCO (Verification of Children Online) project, a cross-sector esearch initiative undertaken in partnership between DCMS, HO and GCHQ, exploring the concept of age assurance as a risk-based approach to recognising child users online, without undermining their privacy. The project has engaged with children, parents, industry & regulators and other experts to build a vision for a safer internet for children, and it has produced research into key technologies, data sources, standards and commercial models. Future work will look to develop further the key emerging themes, including guidance on specific high impact safety measures and supporting safety interventions upstream in the design process.

Child online safety

19.The White Paper committed to make the UK the safest place to be online. It also recognised that users want to be empowered to manage their online safety, and that of their children, but there is insufficient support
in place and users currently feel vulnerable online.

20.As part of the overarching mission to protect the rights of users online, the duty of care will enshrine in legislation the requirement for companies to have appropriate and proportionate measures and processes in place to ensure a higher level of protection for children and vulnerable users. The extent of those processes would be correlated with the risk of harm to young people taking place on the site. This provides the most comprehensive approach possible to protecting children from inappropriate content online, and also enables the regulatory framework to deliver the objectives of Part 3 of the Digital Economy Act,. Companies would be able to use a number of methods to protect children, including possibly - but not necessarily - age assurance tools, which we expect will continue to play a key role in keeping children safe online.

Should the government be doing more to help people manage their own and their children’s online safety and, if so, what?

Engagement

21.One of the key themes of our engagement was parents' concerns about the safety of their children online. Parents' groups, especially, considered online safety to be a particular area where parents' confidence needs to be raised. Although parents felt that they know their children best and are therefore usually the best placed to tailor standard advice for them, they also agreed on the need for more advice and education on how to be online safely. Organisations against violence against women and girls (VAWG) argued that education for online safety should focus not only on behaviours to adopt, but also on discouraging adoption of negative behaviours.

Written consultation

22.From those individual respondents using the online portal, there was an almost even split between those who agreed with the question and those who disagreed (49% and 51% respectively). Conversely, this result was very different amongst organisations who responded online, with 95% agreeing that the government should be doing more.

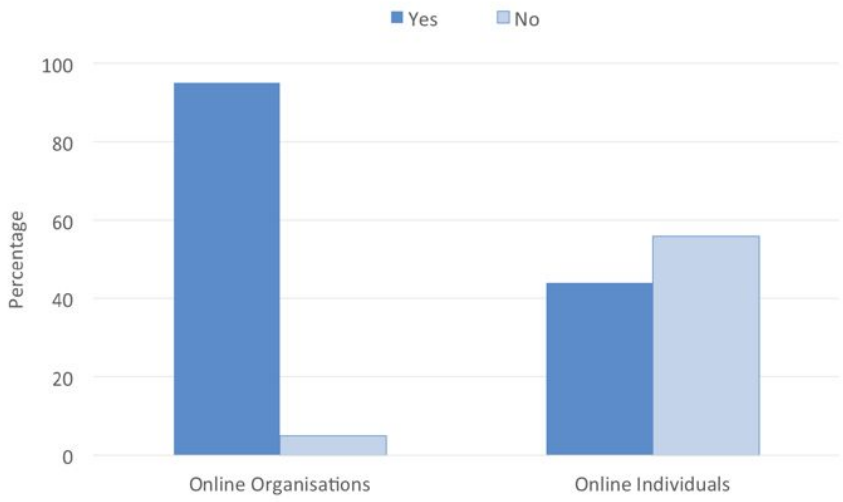

Figure 6: Should the government be doing more to help people manage their own and their children's online safety and, if so, what? Note: Online portal respondents only.

23.Of those who responded "yes" and provided suggestions for what the government should do more of, the most common response was for the government to provide guidance, training and resources. Following this, responses focused on the need to increase education for parents and children. Some responses highlighted other specific areas for intervention looking at increasing and improving education, for example providing resources for teachers and implementing media literacy and privacy education.

24.Other responses included specific suggestions for actions the government should take, for example implementing age assurance measures and increasing the provision and use of family-friendly filters.

25.Some tech companies and civil society organisations, including women's groups and children's charities, agreed that there should be a role for the regulator to play in empowering and educating users. Likewise, many respondents noted that behavioural changes that prevent the content from coming online in the first place are crucial. Nevertheless, some cautioned against 'blaming the victim', and any empowering methods that might absolve companies of their duties and liability.

26.Other respondents from children and vulnerable groups' charities argued that schools should incorporate digital literacy into their curriculum. Similarly, financial services companies urged economic crime to be included in the national curriculum.

27.A few organisations mentioned that an advisory body of relevant public sector and industry experts such as UK Council for Internet Safety (UKCIS) has value in facilitating communication, anticipating future harms to children online, and coordinating activity to address the complex environment children encounter online.

28.Law enforcement organisations suggested expanding the government's Cyber Aware Campaign to cover online abuse and threats, while retaining information about cyber security and crime.

29.Although written consultation responses highlighted some mixed views on the issue, overall the feedback gathered across both a large proportion of responses and in our engagement points to a strong appetite for more support from the government in helping users feel empowered in managing their safety and that of their children.

Education & Awareness

30.The White Paper committed to make the UK the safest place to be online. It also recognised that users want to be empowered to manage their online safety, and that of their children, but there is insufficient support in place and users currently feel vulnerable online.

What, if any, role should the regulator have in relation to education and awareness activity?

31.In the consultation we asked what role, if any, the regulator should have in relation to education and awareness activity. A relatively large proportion of responses, mostly from individuals, stated that the regulator should have no role in education and awareness activity.

32.Education and awareness are key to supporting children to navigate the digital world safely and the statutory relationships, sex and health education curriculum in England will teach them the rules and principles for keeping safe online.

Engagement

33.Throughout our engagement, digital education and awareness were key recurring themes. Some of the industry organisations, as well as children and advocacy groups, emphasised the presence of several existing online safety education programmes and questioned whether the regulator's role would be to reduce or streamline what is already there to improve quality. Many felt that the regulator could have an important role in creating a framework for evaluating the impact of existing education and awareness activity. Others recognised that there could be a role for the regulator or for government in supporting the most vulnerable children. Some also proposed a potential role for the regulator in disseminating alerts about emerging online threats for young people.

Written consultation

34.Of the written consultation responses which agreed the regulator should have a role, many responses suggested it should provide information, advice and guidance, and should work to protect and educate all users.

35.Many responses suggested the regulator should work with other organisations, institutions or government departments to jointly improve education materials and the online safety curriculum, with a number focusing on a need for increased education for children. Additionally, responses stated that the regulator should work to quality assure educational materials and ensure companies fund educational programmes.

36.In line with this, among organisations, respondents from different sectors suggested that the regulator create a national awareness-raising campaign with calls to action for citizens of all ages and technical abilities, including children, teenagers, parents and other adults.

37.Advocacy organisations also argued that via the regulator the government should play a role in making the public aware of how companies are regulated and what their rights and protections are.

38.Overall, while some respondents felt that the regulator should not have a role in education and awareness, others made a range of suggestions for how the regulator might take specific action, including: overseeing industry activity and spend; creating an evaluation framework for assessing education and awareness activity and promoting awareness of online safety.