Written evidence submitted by the Department for Digital, Culture, Media and Sport and the Home Office

9 September 2021

Evidence to:

1) THE DCMS SUB-COMMITTEE ON ONLINE HARMS AND DISINFORMATION

OVERVIEW

1. The Government is pleased to respond to the inquiries from the Joint Pre-Legislative Scrutiny Committee on the Draft Online Safety Bill and the DCMS Sub-committee on Online Harms and Disinformation. Given the similar topics of the inquiries, and our wish to share information openly with both committees, this is a joint response to both calls for evidence.

2. The government published the draft Bill on 12 May 2021, and will prioritise its introduction following pre-legislative scrutiny, as soon as Parliamentary time allows. In developing the Bill and the policy underpinning it, we have been conscious of the complexities of legislating in this space, and have carried out significant public and stakeholder consultation. The policy development phase included a comprehensive 12 week consultation on the Online Harms White Paper, during which we received thousands of responses and held consultation meetings with a wide range of key stakeholders. The full government response to the consultation was published in December 2020 and set out more detail on how these measures would work in practice.

3. The government is also working on measures to support the implementation of the legislative framework, to help users and businesses to manage online safety. In July 2021 the government published the Online Media Literacy Strategy, setting out our ambitions to empower users with the skills and knowledge they need to make informed and safe choices online. This was accompanied by the first annual Online Media Literacy Action Plan, which announced eight government-led initiatives to bring the Strategy to life.

OBJECTIVES

Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

4. The Online Safety Bill aims to make the UK the safest place in the world to be online through three key principles:
    a. **Protecting children**. The strongest protections from harmful or inappropriate content in the Bill will be for children. Tech companies will need to do more to prevent children from being exposed to harmful content or activity such as pornography, grooming, bullying, or content promoting self-harm or suicide.

b. **Tackling criminal activity** - there will be no safe space for criminal content online. This means less illegal content online - such as terrorist material or child sexual abuse and exploitation - and when it does appear it will be removed quicker. For priority illegal content, the regulator will place an emphasis on platforms being proactive, rather than just taking content down once the harm has occurred.
c. **Protecting freedom of expression.** The major platforms will no longer be able to arbitrarily remove controversial content, as they can today. Category 1 platforms (those with the highest reach and highest risk functionalities) will need to be clear what harmful content accessed by adults is acceptable on their services (for example, whether they allow graphic self-harm imagery or some types of online abuse), and enforce their terms and conditions consistently. If they fail to do this, Ofcom can issue hefty fines. The rules will help to unleash a new wave of digital growth by building trust in tech businesses and helping adult users of online sites to make informed choices about the content they wish to be exposed to.

5. The approach in the Bill is focused on the systems and processes which service providers have in place to keep users, particularly children, safe on their services. It does not focus on the removal of individual pieces of content. In this way, the new regulatory framework will increase the responsibility that services have in relation to online safety, and protect freedom of expression. This model will incentivise regulated services to take a risk-management approach to tackling harmful online activity, such as grooming, sharing of terrorist content, or the horrific racist abuse which has recently been seen against footballers competing in the Euro 2020 Championships.

6. The regime will apply to user to user services (those which allow a user of an online service to upload, share or generate content that could be encountered by other users, e.g. social media sites, online marketplaces, or forums), and to search services (search engines). Providers will need to act where their services pose a significant risk of harm to users in the UK. This means that high-reach, high-risk services will have additional responsibilities. On the other hand, the regulatory burden on a low-risk platform with few UK users will be minimal.

7. Regulation has been designed to ensure all services play their part in protecting UK users, while ensuring that requirements are risk-based and proportionate. Harm can occur on services of all sizes, including those without large audiences. Harmful content and activity can also migrate quickly across services. The online safety regulatory framework is comprehensive and designed to remain effective as platforms, technology and the harms landscape evolve.

8. The online safety regime will be regulated by Ofcom. Ofcom is a well-established regulator, experienced at delivering challenging, high-profile roles across a range of sectors. The technological revolution of traditional industries has meant that digital and online services have increasingly become part of Ofcom's existing remit and it has developed relationships with many of the key organisations in the online arena. It also has experience in dealing with large numbers of small businesses as a result of

its spectrum licensing duties. Since Ofcom's confirmation as the future regulator, we have been working closely with it to prepare for the new regulatory regime.

How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

9. The three key principles set out above have remained at the heart of the legislation and underpinning policy throughout its development, and the government is taking a proactive approach to keeping people safe online. The use of the terminology 'online harms' and 'online safety' does not reflect a shift in the focus of the regulation. The new regulatory framework will improve online safety by tackling harmful content online and incentivising a safety by design approach. The Bill will also empower users through protecting freedom of expression, strengthening user rights and redress, and supporting Ofcom's existing duties promoting media literacy.

Will the proposed legislation help to deliver the policy aim of using digital technologies and services to support the UK's economic growth? Will it support a more inclusive, competitive, and innovative future digital economy? Will the regulatory approach in the Bill affect competition between different sizes and types of services?

10. The Government's recently published Plan for Digital Regulation sets out our vision to drive growth and innovation through our regulation of digital technologies, while minimising harms to the economy, security and society. It stresses that, where regulation is necessary it must be streamlined, proportionate, and minimise unnecessary burdens on businesses. The Online Safety Bill is a key part of this wider plan.

11. At its heart, this Bill is intended to restore trust in technology and therefore drive digital growth. Evidence suggests that some people and groups are changing their use of digital services and are decreasing online participation on some services (such as social media) as a result of their exposure to online harms, which creates a challenge for businesses wanting to grow in this space. For example, the 2017 Annual Bullying Survey found that 26% of respondents who had experienced cyberbullying deleted their social media profile, and 24% stopped using social media as a result[1][2]. Online harm can particularly affect certain groups. Findings of the Online Hate Crime Report 2020 indicate that just under 80% of LGBT+ respondents had experienced online abuse in the last 5 years, with 38% of those reducing the use of their online accounts as a result of the most serious incident[3][4]. In addition, a 2020

[1] 2017 was the last edition of the Annual Bullying Survey which included more detailed data on the impacts of cyberbullying specifically. The impact of bullying in general is included in the 2020 Annual Bullying Survey; however, this does not distinguish between cyberbullying and other forms of bullying.

[2] The Annual Bullying Survey - Ditch the Label 2017

[3] https://galop.org.uk/resource/online-hate-crime-report-2020/

[4] The Online Hate Crime 2020 report is a survey of 700 members of the LGBT+ community. Findings should not be used to compare abuse levels with groups outside of the LGBT+ community and given the potential for sample bias from non-probability sampling, may not be representative of the wider LGBT+ community. However, non-probability sampling is often the only option for research with LGBT+ populations.

survey by Plan International showed that after experiencing online violence, around one in five girls[5] left or significantly reduced their use of the social media platform on which it happened[6]. The Online Safety Bill aims to ensure everyone can engage in digital life without being exposed to online harm.

12. In addition to improving safety, the Bill takes a proportionate and risk-based approach, putting the greatest onus on those platforms which have the highest reach or the highest-risk functionalities. The structure of the Bill's provisions ensures that regulatory expectations on services are reasonable and proportionate to the severity of the potential harm posed and the size and capacity of the business. In the full government response, we announced that low risk businesses - such as those websites that only allow user reviews on products and services - would be out of regulatory scope. As a result of this exemption, the websites of many small businesses for which the only in-scope functionality is the ability to leave a user review will be taken out of scope. The framework is designed to target those services where the greatest reduction in harm facilitated by user-generated interaction online can be achieved. Overall we expect fewer than 3% of UK businesses to be in-scope of regulation.

13. The online harms regulatory regime will also support the development of the safety technology sector, as effective online safety technologies will play a key role in enabling service providers to comply with their duties of care and keep users safe. The UK's leading online safety technology sector spans an impressive range of technologies, including age assurance technologies that enable a company to know the true age of its users, and Artificial Intelligence that can detect child sexual abuse material, spot disinformation content, and remove bad actors from online communities. The safety technology sector has seen an annual growth rate of 35% in recent years, with revenues expected to exceed £1bn by the mid-2020's. Internationally, UK companies have around 25% of the global market share[7].

14. In parallel with progressing the Online Safety Bill, the government will continue to work closely with the technology sector, academia and civil society to make the UK a world leader in online safety technologies. Over the last year we have founded the Safety Tech Innovation Network, supported the creation of the Online Safety Tech Innovation Association (OSTIA), and hosted the world's first safety tech expo in collaboration with CogX which brought together globally recognised leading voices from the sector. We have published reports including an annual sectoral analysis, and have carried out several online events on topical issues designed to boost awareness and bring the sector together. Our future work will include a focus on funding for companies to help find safety tech solutions to high profile challenges, and hosting the first ever Safety Tech Summit, at which G7 countries will be represented.

---

[5] The survey received over 14,000 responses from girls aged between 15 and 25.

[6] Free to be online: A report on girls' and young women's experiences of online harassment - Plan International 2020

[7] Safer technology, safer users: The UK as a world-leader in Safety Tech - DCMS 2020

Are children effectively protected from harmful activity and content under the measures proposed in the draft Bill?

15. The strongest protections in the draft Bill are for children. All service providers in scope will need to do far more to protect their users, including children, from being exposed to illegal content or activity on their services. In addition, providers of services which are likely to be accessed by children will be required to have systems and processes in place to protect children from content or behaviour which is harmful to them but is not illegal (for example, pornography).

16. All service providers in scope will need to carry out an assessment of whether their platform is likely to be accessed by children. This will cover both whether it is possible for children to access the service, or any part of it, and whether a significant number of children use the service or are likely to be attracted to it.

17. Services which do not consider they need to implement the higher level of protection for children will need to be able to provide robust evidence to the regulator that children are not accessing their service, and keep this assessment under review. The legislation particularly requires service providers to carry out a new assessment on the likelihood of children's access before making significant changes to the design or operation of the service, or if the company is aware of evidence suggesting either that there has been a significant increase in the number of children using the service or that the effectiveness of systems in place to prevent children accessing the service is reduced. Any service which does not carry out a child access assessment will be treated as likely to be accessed by children until an assessment has been completed which demonstrates that they are not.

18. The protections for children are based on risk assessments, tailored to the individual platform and its functionality. Service providers which are likely to be accessed by children will be required to assess the risk their service poses for children, put in place proportionate measures to protect children from those risks, and monitor the measures for effectiveness. They will have a duty under the legislation to undertake these risk assessments regularly, including considering how the design and operation of the service may increase or reduce the risks identified. Ofcom will set out the steps companies can take to protect children on their services so there should be a consistent approach across service providers. In practice, we expect companies to take steps to ensure that children are not able to access services that pose the highest risk of harm to them, such as online pornography and dating sites. We also expect companies to take steps to ensure that children can use their services safely. This would include protecting children from harmful content and activity, ensuring that systems for targeting content to children (such as the use of algorithms) protect them from harmful material, and reviewing children's use of higher risk features such as live streaming or private messaging (including encrypted messaging).

19. In recognition of the fact that content which may be harmful to younger children will not necessarily be harmful for older children to access, companies will be required to

assess the risks their services pose to children of different ages and provide age-appropriate protections. Ofcom will also be required to have regard to the fact that children have different needs at different ages when preparing codes of practice relevant to the protection of children.

20. In addition to having systems and processes in place to protect children from harmful content and behaviour online, service providers will need to be more transparent and accountable to child users and their parents and carers. For example, Category 1 services will be required to provide annual transparency reports containing information about the steps they are taking to tackle online harms, which may include information about how they are delivering a higher level of protection to children. The Secretary of State will have the power to set additional thresholds to bring other services (such as search engines) into scope of the transparency reporting requirements if necessary. Services will also be required to have clear and accessible ways for users, including children or their parents and carers, to report harmful content. This approach will help children and their parents and carers make informed decisions about the services they use, and will allow Ofcom to highlight best practice among platforms and build an understanding of the risks across the sector more widely.

21. Providers of services will be required to take particularly robust action to tackle online child sexual exploitation and abuse (CSEA) content. This includes using proportionate systems and processes to minimise the presence and dissemination of CSEA content, and ensuring that reports of CSEA content are acted upon swiftly. Ofcom will have the power to require a company to use automated technology to identify and remove CSEA content from its service. This power is subject to stringent safeguards to protect user privacy, and can only be used when doing so is the only effective and proportionate action available. Ofcom will only be able to require the use of highly accurate technology that meets minimum standards, and it must have evidence of persistent and prevalent content. These measures will help ensure there is no safe place for online offenders and that platforms and search services are doing all they can to protect victims and potential victims of this crime. Further, the government is considering introducing a requirement for companies to report child sexual exploitation and abuse identified on their services to a designated body. This could help to protect victims of online CSEA by ensuring law enforcement have the information they need to identify offenders and safeguard children.

22. The government expects Ofcom to prioritise enforcement action that will ensure the strongest protection possible for children. Ofcom will be required to set out in enforcement guidance how it will take into account any impact on children due to a company's failure to fulfil its duties of care. In setting its guidance and ways of working, Ofcom will be required to consult with a range of interested bodies and stakeholders, including those representing the interests of children. We also expect Ofcom to consult with users to ensure it understands their experiences, detects issues early and is able to address their concerns. We are looking at the best ways to ensure that Ofcom has the powers available to it to carry out these user advocacy functions.

Does the draft Bill make adequate provisions for people who are more likely to experience harm online or who may be more vulnerable to exploitation?

23. The online safety proposals will considerably improve the online experience for children and vulnerable users. The draft Bill will be particularly beneficial for those who are currently more likely to experience harm associated with content or activity online. For example, disabled users, women and black and minority ethnic users may be more likely to suffer abuse online. Adults with mental health conditions may be more likely to view self-harm or suicide content.

24. All service providers in scope of the framework will need to have robust systems and processes in place to tackle illegal content, which may be even more harmful when encountered by a vulnerable person. Terrorist groups and individuals use the internet to spread propaganda designed to radicalise, recruit and inspire people, and to incite, provide information to enable, and celebrate terrorist attacks.

25. Category 1 service providers will also be required to undertake regular risk assessments to identify the risk of harm posed by a broader range of content on their services, which does not meet the threshold for a criminal offence. Priority categories of such content for adults will be set out in secondary legislation. These are likely to include the most prevalent forms of online abuse, together with other harmful material which might disproportionately impact vulnerable users, such as self-harm or suicide content. The risk assessments that companies will be required to carry out will need to take into account the user base of the service in question and consider the nature and severity of harm that might be suffered by adults. Service providers will also need to consider whether content might particularly affect a particular group of people or people with a shared characteristic.

26. Following the risk assessment, Category 1 service providers will need to set out clearly in their terms of service what legal but harmful content, such as the promotion of self-harm, is acceptable on their service(s), and enforce that consistently and transparently. Service providers must ensure that their terms of service are clear and accessible. This will make it much easier for vulnerable adults or, where relevant, their carers, to understand which online services may be most appropriate for their needs.

27. Vulnerable users will also have access to the reporting and redress mechanisms established in the draft Bill. In-scope companies will be required to put in place reporting and complaints mechanisms that are easy to access and use. The Bill also includes provision for affected persons who are not users of a service to access these mechanisms, including those who are targeted or are members of a group targeted by a piece of content, and those who are assisting a user, such as a vulnerable adult, who needs help to complain.

28. Ofcom will also be given the power to require a company to use automated technology to identify and remove terrorist content from their public channels and CSEA content from any part of the service. These powers can be used when it is the only effective and proportionate and necessary action available, and they are subject to strict safeguards. Ofcom will only be able to require the use of highly accurate technology that meets minimum standards and it must have evidence of persistent and prevalent terrorist content (on public channels) or CSEA content on (any part) of a service. Ofcom must also be clear that other measures could not be equally effective.

29. Ofcom's existing statutory duty under section 3(4) of the Communications Act 2003 will apply in relation to its new safety functions under the online safety regime. This requires Ofcom to consider (i) the vulnerability of individuals whose circumstances appear to put them in need of special protection and (ii) the needs of people with disabilities, the elderly and those on low incomes, when performing its functions.

Is the "duty of care" approach in the draft Bill effective?

30. In the draft Bill, the 'duty of care' is a term used to describe the duties placed on service providers to make them more responsible for their users' safety. The duty of care can broadly be split into two components: risk assessments and safety duties. Service providers will be required to understand the risk of harm to their users, and then put in place systems and processes to improve user safety which are appropriate for their services. In order to help companies comply with their safety duties, the duty of care places an obligation on Ofcom to produce codes of practice to outline the steps providers can take to comply with their duties.

31. The draft legislation contains specific duties of care to assess risks and address illegal content, content that is harmful to children and content that is harmful to adults. Cumulatively these duties cover the same elements as the overarching duty of care initially proposed in the Online Harms White Paper. However, more specific duties will give companies and Ofcom greater legal certainty and direction about the regime. In turn this will make it easier for Ofcom to effectively enforce against non-compliance.

32. This approach underpins the risk-based and proportionate regulation that the diverse, dynamic and innovative online sector requires. It gives companies real responsibility for the risks and impacts that their services have on their users' safety, and obligations to address these effectively, without imposing disproportionate burdens. Ofcom will consult extensively on their codes of practice setting out the steps companies can take to comply with their duties, and will be able to update the codes to cover new types of services or technology. This flexibility to update the measures in the codes which can be taken to achieve the safety duties future-proofs the regulatory framework. Overall the provisions in the draft Bill have been designed to drive the systematic improvements necessary to improve user safety, while protecting freedom of expression and the benefits for users associated with the digital economy.

Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content?

- **What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?**
- **Does the draft Bill focus enough on the ways tech companies could be encouraged to consider safety and/or the risk of harm in platform design and the systems and processes that they put in place?**

33. The regulatory framework set out in the draft Bill is entirely centred on systems and processes, rather than individual pieces of content, putting these at the heart of companies' responsibilities. In carrying out risk assessments, companies will be required to consider the risk of users encountering illegal or harmful content through their services, including the part played by the services' algorithms and systems for disseminating content. They will have to look at how the design of their service and its functionalities, as well as how the service is operated, affects the presence and spread of illegal or harmful content.

34. Companies' safety duties for illegal content and content that is harmful are also framed around systems and processes. User-to-user services will be required to operate their services using proportionate systems and processes to minimise the presence, duration and spread of illegal content and to remove it swiftly once they are aware of it. Search services will be required to put in place proportionate systems and processes designed to minimise the risk of individuals encountering illegal content in or via search results. Companies will also be required to provide age-appropriate protections for children using their services and monitor these for effectiveness. As set out in paragraph 20, Ofcom will also be able to require companies to use automated technology to tackle terrorist or CSEA content where specific criteria have been met.

35. The focus on robust processes and systems rather than individual pieces of content has a number of key advantages. The scale of online content and the pace at which new user-generated content is uploaded means that a focus on content would be likely to place a disproportionate burden on companies, and lead to a greater risk of over-removal as companies seek to comply with their duties. This could put freedom of expression at risk, as companies would be incentivised to remove marginal content. The focus on processes and systems protects freedom of expression, and additionally means that the Bill's framework will remain effective as new harms emerge. The regulator will be focused on oversight of the effectiveness of companies' systems and processes, including their content moderation processes. The regulator will not make decisions on individual pieces of content, and will not penalise companies where their moderation processes are generally good, but inevitably not perfect.

36. Setting prescriptive standards for all companies would not be compatible with a proportionate and risk-based system. Instead, Ofcom will set out steps in codes of practice that companies can take to comply with their duties. These codes are likely to place a high level of importance on a safety by design approach, the use of

algorithmic recommendations, and safer default settings in companies fulfilling their safety duties. The government published new, voluntary safety by design guidance on 29 June 2021. This will help companies - smaller companies and start-ups in particular - design and build online services that are safer for their users and help them to take steps towards adopting a safer design approach in advance of legislation. The government also published the interim codes of practice on terrorist content and child sexual exploitation and abuse online in December 2020. The interim codes set out the Government's expectations of what companies should be doing to address terrorist content and activity and CSEA online, providing clarity to companies in the interim between now and when the regulator is established and able to issue their own codes.

How does the draft Bill differ to online safety legislation in other countries (e.g. Australia, Canada, Germany, Ireland, and the EU Digital Services Act) and what lessons can be learnt? What are the lessons that the Government should learn when directly comparing the draft Bill to existing and proposed legislation around the world?

37. Online safety is a global issue and it is important that we continue to collaborate internationally to tackle the issue of harm online. Like the UK Government, many other like-minded countries are developing their own approaches to improve internet safety, including through regulatory frameworks. We have continued to look across the international landscape to learn from the experiences of our international partners, including undertaking continued stakeholder engagement on issues of concern.

38. The German NetzDG regulations, introduced in 2017, provided an opportunity to consider an existing regulatory approach. These regulations require large social media companies to remove "obviously illegal" speech within 24 hours of it being reported. This differs from the approach the UK has taken in the draft Online Safety Bill, which does not have a focus on the removal of individual pieces of content, and instead introduces duties of care requiring companies to implement appropriate systems and processes to mitigate and manage the risk of harm arising from their services.

39. The EU published its draft Digital Services Act on 15 December 2020, which, like the draft Online Safety Bill, sets out new expectations on companies to ensure they have proportionate systems and processes in place to mitigate risks and keep their users safe online. Under both approaches, in-scope platforms will need to conduct risk assessments, tackle illegal content on their platforms, and enforce their terms and conditions consistently and transparently.

40. There are however some key differences between the two approaches, including that the draft Online Safety Bill has a focus on online child protection. Advertising and consumer standards are not covered by the draft Online Safety Bill, to avoid duplicating regulatory requirements which already exist for both advertising and consumer standards, and the Government is carrying out separate work to address concerns in these areas. The Department for Business, Energy and Industrial

Strategy is currently developing proposals to address subscription traps and other consumer protection measures. Following a call for evidence last year, DCMS will be launching a consultation as part of the Online Advertising Programme before the end of the year.

41. We have also been following the progress of legislation as it develops in a number of other countries, including the Australian Online Safety Bill, the Irish Online Safety and Media Regulation Bill and France's new legislation, in place of the earlier Avia law. These proposals seek to introduce new provisions to promote online safety, impose obligations on social media companies and introduce an independent regulator to oversee their implementation. The approach of these laws is similar to that of the UK in seeking to promote online safety while protecting freedom of expression and democratic principles online. However, there are a number of variations amongst these proposals. For example, the UK's Online Safety Bill specifically excludes low risk services from its scope to ensure a proportionate and risk-based approach. Other countries, like Canada, are preparing to introduce similar legislation, and we continue to engage with them to share our approach.

42. We believe that our approach strikes the right balance, providing a holistic solution to tackling online harms by addressing both illegal and legal but harmful material online, and establishing duties of care that companies owe their users, overseen by an independent regulator. Our approach can lead towards new, global approaches for online safety that supports democratic values. As part of our global strategy for tackling online harms, the UK Government will continue to work with international partners, industry and civil society to identify best practice, build consensus and seek common approaches to keep citizens safe online. Through the UK's presidency of the G7, we are bringing countries together to promote proportionate and risk-based solutions to address harmful online activity that uphold our shared values. We look forward to continuing to share experiences on our approach and continue to welcome views from our partners internationally on this and on how we can best continue to work together to deliver effective global approaches.

Does the proposed legislation represent a threat to freedom of expression, or are the protections for freedom of expression provided in the draft Bill sufficient?

43. The protection of freedom of expression is one of the core objectives of the Bill. By promoting an online environment where people will be able to contribute without fear of abuse, and where major platforms will be held accountable for their decisions on removal of content, the Bill will improve freedom of expression online over the current status quo.

44. Importantly, the Online Safety Bill does not require service providers to remove any legal content. Category 1 companies (those with the highest risk and reach) will need to risk-assess for content that poses a material risk of having - or indirectly having - a significant adverse physical or psychological impact on an adult of ordinary sensibilities, and then set terms and conditions relating to that content. The service providers will have discretion as to the nature of these policies. For example, they could choose to tolerate the content, but must make this fact clear and accessible to

users. They could also provide users with tools to manage their own exposure to content that is accepted on a service but may be harmful. This will allow adult users to make informed decisions about the types of content that they are willing to risk being exposed to before using a site.

45. Once a service provider has set its terms and conditions, it must then enforce these policies consistently, and would not be able to arbitrarily remove content. Platforms will be required to provide users with effective mechanisms to seek redress if they believe that content has been removed unfairly. This is a major improvement on the status quo whereby users complain about the opaque, arbitrary removal of their legitimate content and the lack of clear routes to appeal the takedown.

46. The Bill contains a number of specific protections for freedom of expression online. Its provisions mitigate the risk that service providers interpret their obligations in an overly restrictive way by imposing a duty on in-scope companies to consider the importance of protecting users' rights to freedom of expression when fulfilling their safety duties and user redress duties. Category 1 service providers will need to assess the impact that their safety policies and procedures could have on freedom of expression, and publish a statement setting out that impact and any positive steps that have been taken to mitigate risks to freedom of expression. Ofcom will also need to carry out its new functions in a way that protects freedom of expression. The Bill also includes protections for journalistic content and for content of democratic importance to safeguard pluralism and media freedoms, and to ensure internet users can continue to engage in robust debate online. These provisions are discussed in more detail in paragraphs 53 - 56.

What are the key omissions to the draft Bill, such as a general safety duty or powers to deal with urgent security threats, and (how) could they be practically included without compromising rights such as freedom of expression?

47. We have developed the draft Bill to make sure the regulation is coherent, proportionate and agile in response to evolving risks and digital technologies. The regulatory framework sets out a comprehensive and coherent set of specific duties covering, for example, risk assessment, safety measures, reporting and redress and record-keeping. The approach taken will effectively tackle illegal content, protect children from content that is legal but harmful to them, and ensure that adults are able to take informed decisions about potential exposure to content that is legal but harmful when accessing Category 1 sites. The regulatory framework is designed in a way that is future-proofed and technology-neutral, to ensure that it remains relevant and effective as technologies evolve. We do not agree that there are omissions in the Bill.

CONTENT IN SCOPE

Is it necessary to have an explicit definition and process for determining harm to children and adults in the Online Safety Bill, and what should it be? What would be a suitable threshold for significant physical or psychological harm, and what would be

a suitable way for service providers to determine whether this threshold had been met?

48. The draft legislation already defines the harmful content and activity covered by the duties of care. This includes illegal content, content that is harmful to children and content that is harmful to adults. Priority content in each of these categories will be set out in legislation.

49. The legislation sets out that legal material that is harmful to children or adults should be in scope where the service provider has reasonable grounds to believe that the content gives rise to a *material* risk of a *significant* adverse physical or psychological impact on an individual of ordinary sensibilities, or on a particular individual about whom the provider has specific knowledge. This impact could be by the content indirectly resulting in physical injuries or by having a significant negative effect on an individual's mental state. That could include fear, anxiety, depression, stress and other medically recognised mental illnesses. Additional provision is made in relation to cases where content is likely to particularly affect people with a certain characteristic or who belong to a certain group, and where the provider has relevant knowledge about a particular child or adult concerned by the content. Priority legal but harmful content will be set out in secondary legislation, but illustrative examples which would fall into each of these categories could include e.g. content relating to suicide or self-harm; online abuse and cyber-bullying; and racist abuse or abuse targeted at individuals with a disability.

50. This test does not include all content that might have a physical or psychological impact on an individual. Instead it sets a high threshold to ensure that merely upsetting, trivial content, or indeed rude and controversial content, is not captured by the regulatory regime. The test, however, does not require the adverse psychological impact to be a recognised mental illness as this would be too high a bar, meaning that service providers would not have to address content that is widely recognised as harmful such as online abuse. The main forms of legal but harmful content, informed by this test, will be designated as priority harmful content in secondary legislation. This will allow for parliamentary oversight and democratic debate about the harms to be included in the list. The Government will be responsible for establishing the list of priority harms that companies must address, taking into account advice from Ofcom about the evidence of the prevalence and impact of harmful content.

51. All companies whose services are likely to be accessed by children will need to assess the risks of priority and other legal content that meets this test in relation to children appearing on their services and provide age appropriate protections. Category 1 service providers will need to assess the risks of priority and other legal content that meets this test appearing on their services, and set and enforce terms of service which explain how they will address this content. Regulation will not prevent adults from accessing or posting legal content, nor require companies to remove specific pieces of legal content.

The draft Bill specifically includes CSEA and terrorism content and activity as priority illegal content. Are there other types of illegal content that could or should be prioritised in the Bill?

52. Legislation will set out categories of priority illegal content. The White Paper set out an initial list of harms that the government envisaged being in scope of the framework, including extreme pornography, incitement to violence, harassment and several others. The legislation will also list priority content that is harmful to children, and priority content that is harmful to adults. The Secretary of State will be able to update these priority categories through further regulations to ensure that the legislation can adapt to new harms that may emerge in future. This approach balances the need to give certainty to businesses on the harms they must address, whilst ensuring the legislation remains agile and flexible to emerging harms and risks.

53. The Secretary of State must consult Ofcom before designating priority categories of legal content that is harmful to adults and children. So that it can fulfil this consultatory role, Ofcom must carry out reviews of the incidence of content that is harmful to children and content that is harmful to adults, as well as the severity of harm that individuals suffer, or may suffer, as a result of encountering those kinds of content. Ofcom will have to conduct and publish these reviews at least once every three years.

54. Relevant terrorism and CSEA offences are already listed on the face of the Bill. The UK's definition of terrorism includes an act or the threat of serious violence to advance an ideological, religious, racial, or political cause. The Terrorism Act 2000 definition is sufficiently broad to capture modern causes of terrorism, including violence relating to "incel" groups (typically online communities of young men who define themselves by their inability to find a romantic or sexual partner). Online content assessed to be in breach of UK terrorism legislation constitutes illegal terrorist content. For other illegal content, the government will set out priority offences in legislation, requiring platforms to have systems and processes in place to minimise the presence, duration and spread of this content. The Bill sets out that, when deciding whether to designate an offence as a priority offence, the Secretary of State must consider the prevalence of that type of content, the level of risk of harm to individuals caused by that content and the severity of that harm. If an offence is not included on the list of priority offences, this does not mean that the company does not need to address that relevant content - it simply means that the company will have to remove that content as soon as possible once it is aware of the content. This also applies to content linked to priority offences. The government will need to undertake detailed analysis to determine which offences will be designated in the priority list. As a result we cannot at this stage state if any particular offence will or will not be on the priority list.

The draft Bill specifically places a duty on providers to protect democratic content, and content of journalistic importance. What is your view of these measures and their likely effectiveness?

55. The major tech platforms currently exercise significant power over what journalistic content and content of democratic importance appears on their services. Currently, the major tech platforms are able to arbitrarily remove journalistic content and content of democratic importance. Many users, including news publishers, complain about the opaque reasoning given for the removal of their content and a lack of clear routes to appeal.

56. The Bill will address this concern in relation to journalistic content by requiring the relevant companies to put in place protections for journalistic content when it is shared on their services. Firstly, the legislation provides a clear exemption for news publishers' content from the scope of regulated 'user-generated content' as defined by the Bill. This means service providers will not have any new legal duties for these news publishers' content as a result of our legislation. Secondly, the legislation will also include a positive obligation on Category 1 companies to put in place safeguards for all journalistic content shared on their platforms. Journalistic content' includes all content that is created for the purpose of journalism and which is UK-linked. This includes citizen journalists' journalistic content, as well as news publishers' journalistic content. These safeguards will ensure that platforms balance their content moderation objectives with protecting users' access to journalistic content. Further, they will need to offer users expedited appeals processes where their journalistic content is moderated. Service providers will need to be transparent about the systems and processes they have implemented to achieve these objectives. This approach means they can be held to account for the removal of journalistic content, including with respect to automated moderation tools. Therefore the Online Safety Bill represents a significant improvement on the status quo for journalistic content online.

57. There may be very rare instances when journalistic content and content of democratic importance shared on a service poses such a great risk to the platform's users, or is in such clear breach of their terms and conditions, that the service wishes to remove it. For example, journalism showing pictures of deadly violence may not be suitable for a platform with a user base predominantly made up of children. That the removal of such content is allowed is important to ensure that these duties are effective in protecting journalistic content, without requiring that platforms carry content that is of greatest risk to their users. In such instances the platform will need to justify the removals against a clear and properly enforced policy, and make sure users, news publishers and journalists have a swift right of appeal. If they do not, Ofcom will be able to enforce against them.

Earlier proposals included content such as misinformation/disinformation that could lead to societal harm in scope of the Bill. These types of content have since been removed. What do you think of this decision?

58. The government takes the issue of societal harms very seriously. That is why we are taking a range of legislative and non-legislative measures to address this issue. The Online Safety regulatory framework will address some types of societal harm through its duties regarding illegal content - for example, both CSEA content and terrorist material can cause significant societal damage. Other types of societal harm will be

addressed through the duties of care on Category 1 services regarding content that is legal but harmful to individuals. For example, false vaccine information that could cause significant (physical) harm to an individual will be in-scope, but this content could also cause harm to society by eroding public trust in the NHS (which is a type of harm which would not be in scope of the Bill). The Bill will also establish an expert advisory committee on mis/disinformation, and will strengthen the existing Ofcom duty to promote media literacy, which will improve user resilience to mis/disinformation.

59. The duties of care in the Online Safety Bill will not apply to content and activity which only causes harm to society in general, as this could incentivise excessive takedown of legal material due to the lack of consensus about what might result in societal harm.

60. It is essential that these legislative measures uphold and protect freedom of expression online, such that people can express their views on issues that are important to democracy, to promote a thriving democracy. As such, these provisions are proportionate to the risks mis/disinformation pose to users, whilst ensuring these freedom of expression protections are maintained. It is not possible to build trust by stamping out all dissent. To take the coronavirus vaccine roll-out as an example, some people have genuine questions about the vaccine (such as, about how quickly the vaccine was approved). We have good answers to those questions, and should educate people rather than silencing them, as some have called for in trying to legislate against vaccine misinformation.

Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

61. Protecting children from online pornography is a government priority. The online safety regime will capture the most visited pornography sites, video-sharing sites, forums and via image or video search engines, and pornography on social media. Where commercial pornography sites host user-generated content or facilitate online user interactions (including video and image sharing, commenting and live streaming), they will be in scope of the Online Safety Bill.

62. The government expects companies to use age verification technologies to prevent children from accessing services which pose the highest risk of harm to children, such as online pornography. Companies would need to put in place these technologies or demonstrate that their alternative approach delivers the same level of protection for children, or face enforcement action by the regulator. As referenced in the recently published Tackling Violence against Women and Girls strategy, the government recognises the concerns that have been raised about protecting children from online pornography on services which do not currently fall within the scope of the Online Safety Bill, and the DCMS Secretary of State has said that he intends to use the pre-legislative scrutiny process to explore whether further measures to protect children are required.

63. Furthermore, the government has engaged extensively with a broad range of stakeholders, including the financial industry, consumer groups, law enforcement and other public bodies. We have listened to their views carefully, and decided that online fraud should be included in the scope of the Online Safety Bill. This means that service providers in scope of regulation will need to take action to tackle fraud, where it is facilitated through user-generated content. We expect the regulatory framework to have a particular impact on specific types of fraud, such as romance scams, which are estimated to have cost victims over £60 million in the year ending February 2020 and can cause significant psychological harm to victims.[8]

64. The framework focuses on user-generated content, and must remain targeted and proportionate for businesses and Ofcom. Paid-for advertising, including on search engines and social media platforms, will remain outside of scope. We are however deeply concerned about the growth and scale of online fraud, and the devastating financial and psychological impact it can have on individuals. Our Online Advertising Programme will focus on addressing harms caused by the content and/or placement of advertising online. We anticipate that it will include looking at the role advertising plays in online fraud, amongst other things, and the extent to which interventions in the regulation of online advertising could be effective in reducing the occurrence of fraud. DCMS is leading on this programme and will launch a public consultation later this year.

65. However, we know that to tackle the problem of fraud we will need a concerted effort from across Government, law enforcement and the wider public sector as well as the private and third sectors. We recently published a Statement of Progress on our Economic Crime Plan covering action to be taken in the year 2021/22. This confirmed our commitment to develop an ambitious framework for a Fraud Action Plan, covering the years 2022 to 2025.

66. The plan will include the Government working with industry to remove the vulnerabilities that fraudsters exploit, with intelligence agencies to shut down known fraudulent infrastructure, with law enforcement to identify and bring the most harmful offenders to justice, and with all partners to ensure that the public have the advice and support they need. The Fraud Action Plan is now being developed and will be published after this year's spending review.

Are the definitions in the draft Bill suitable for service providers to accurately identify and reduce the presence of legal but harmful content, whilst preserving the presence of legitimate content?

67. As set out above, it is important to note that regulation will not prevent adults from accessing or posting legal content, nor require service providers to remove specific pieces of legal content. We believe that the legislation provides suitable definitions of legal content that is harmful to children or harmful to adults to enable companies to fulfil their duties. Category 1 companies will have duties in respect of legal content that is harmful to adults where there is a material risk of the content having, or

[8] National Strategic Assessment of Serious and Organised Crime - 2020

indirectly having, a significant adverse physical or psychological impact on an adult of ordinary sensibilities. Categories of priority content that is harmful to adults will be set out in secondary legislation, following advice from Ofcom.

68. On preserving legitimate speech, Category 1 service providers will not be able to arbitrarily remove legal content that is harmful to adults. Instead, those companies will need to set out clearly in their terms of service whether the content is allowed on their platform and how it will be treated if so, and enforce those terms consistently. This will mean that they will no longer be able to arbitrarily remove content, including where it expresses controversial viewpoints. The approach will also enable adult users to make informed choices about the services they use and the harmful content that they are willing to risk being exposed to.

69. One of the overarching principles of our framework is to protect users' right to freedom of expression online. Further protections for freedom of expression are built into the legislative framework through the fact that all service providers will have to consider and implement safeguards for freedom of expression when fulfilling their duties. Category 1 service providers will have additional duties to assess their policies' impact on users' right to freedom of expression and to take steps to mitigate this impact. As a public authority subject to the Human Rights Act 1998 Ofcom will also have to fulfil its new functions in a way that protects freedom of expression. Users will also be better able to complain and seek action from a platform if they believe their content has been unfairly removed from a platform.

SERVICES IN SCOPE

The draft Bill applies to providers of user-to-user services and search services. Will this achieve the Government's policy aims? Should other types of services be included in the scope of the Bill?

70. The Online Safety Bill applies to providers of user-to-user services and search services. The service providers in scope of the regulatory framework are those that have control over how the content on a service (or the content which is found via a service in the case of search services) is encountered and treated. These providers are best placed to ensure that harm is tackled effectively. The legislation is designed to ensure that companies take appropriate responsibility for the harm arising from their services, even when they are not liable for each individual piece of user-generated content.

71. Certain other services which give rise to a low risk of harm, such as email services and internal-business services, are exempt from the scope of the Online Safety Bill to ensure the framework is risk-based and proportionate. Some internet infrastructure providers, such as internet service providers and browsers, also have an important, albeit different, role to play in combating online harms, including child sexual exploitation and abuse. In the full Government response to the Online Harms White Paper consultation, the government committed to publishing voluntary guidance for infrastructure providers, setting out where their actions can help identify and prevent child sexual exploitation and abuse.

72. Similarly, internet infrastructure providers will play a part in implementing the 'access restriction orders' that Ofcom can pursue under the Bill. Where there is serious ongoing harm to UK users, and it is appropriate and proportionate to do so, Ofcom can apply to the Courts for access restriction orders to be issued to third parties (such as internet infrastructure providers) to restrict or impede access for UK users to a non-compliant service. The Courts will weigh up the rights of all involved parties before issuing an order. We expect these orders to only be pursued in the most serious cases of user harm.

The draft Bill sets a threshold for services to be designated as 'Category 1' services. What threshold would be suitable for this? Are the distinctions between categories of services appropriate, and do they reliably reflect their ability to cause harm?

73. Under the online safety framework, only Category 1 service providers will have duties in relation to legal but harmful content accessed by adults, such as racist abuse. All service providers in scope will need to fulfil duties in relation to illegal content and to protect children (if their service is likely to be accessed by children). The distinction between duties on Category 1 and other services will protect freedom of expression and mitigate the risk of disproportionate burdens on small businesses. It will also ensure that companies with the largest online presence are held to account, addressing the mismatch between companies' stated safety policies and many users' experiences online.

74. The thresholds for Category 1 designation will be informed by research carried out by the regulator, Ofcom. Thresholds will relate to the functionality, such as live-streaming, and number of users of a service. Therefore, the services that will be designated as Category 1 will be limited to the platforms that pose a significant risk of harm to adult users. Although the thresholds have not yet been determined, we expect Category 1 to include a small number of platforms.

75. The proposed system to designate Category 1 services is flexible and agile, ensuring that if a new or existing service meets the threshold criteria they can easily be added to the register. In addition, the thresholds can also be updated over time to ensure they continue to capture the highest risk services.

ALGORITHMS AND USER AGENCY

What role do algorithms currently play in influencing the presence of certain types of content online and how it is disseminated? What role might they play in reducing the presence of illegal and/or harmful content? Are there any foreseeable problems that could arise if service providers increased their use of algorithms to fulfil their safety duties? How might the draft Bill address them?

76. Algorithms are one of the systems and processes used by many companies to operate their services, and it is recognised that they can influence the spread of harmful content online. Research commissioned by 5Rights indicates that the use of algorithms which amplify the type of content on social media platforms that a profile appears to show interest in can potentially result in the promotion of harmful content

to children. The report used child-aged avatars to assess which content the algorithms amplified, which they claim worryingly included sexualised images, content promoting eating disorders or weight loss, and self-harm, despite the platforms recognising that these accounts were registered as children.[9]

77. There are many benefits in using algorithms for safety tech purposes. Human moderation alone cannot keep pace with the volume of harmful content online, and AI based algorithms help companies detect and then block or filter harmful content at scale. However, there are also considerations which must be taken around the use of algorithms for user safety. Algorithms themselves are only as useful as the data they are based on. Historically, it has been shown that where data contains bias, the algorithms will reproduce that bias in its results. For example, algorithms may inadvertently perpetuate harmful biases, and exclude or disproportionately impact certain groups, thereby perpetuating harm themselves. There are potential ethical and exclusion implications that are already being considered by those developing AI based safety technologies.

78. This is why the Online Safety Bill requires companies to consider the impact of algorithms as part of their risk assessments and in carrying out their safety duties for illegal content and content that is harmful to children. Ofcom will publish guidance for companies on carrying out risk assessments and set out how companies can fulfil their safety duties in codes of practice, both of which will be able to cover the role of algorithms.

79. Ofcom will have a range of powers at its disposal to help it assess whether companies are fulfilling their duties, including in relation to their algorithms. Ofcom will have the power to require information from companies as well as powers to require interviews, require regulated service providers to undergo a skilled persons report, and in certain circumstances, the power to access premises, data and equipment. Ofcom will also be able to require companies to include information about the steps that companies are taking to deal with illegal and/or harmful content (including systems and processes for identifying such content) and information about the steps that companies are taking to protect freedom of expression online, in their transparency reports. These powers will ensure Ofcom are able to build their understanding about the role that algorithms can play in relation to dealing with harmful content online.

Does the draft Bill give sufficient consideration to the role of user agency in promoting online safety?

80. The draft Bill will ensure that online service providers are held accountable for keeping their users safe from harmful, user-generated content. However, we recognise that there is a shared responsibility for safety online between government, companies, and the users of services. To be able to carry out their role in this effectively, citizens must have the skills and knowledge to be able to reduce their

[9] Pathways: How digital design puts children at risk (5Rights, 2021)

interaction with harms online and, if they do encounter harm, know how to respond appropriately (e.g. reporting online abuse).

81. It is not always clear to users how privacy or other settings can be used to decrease risks online. To support users in this, Ofcom will have an enhanced duty to promote media literacy relating to both offline and online channels. This will include carrying out, commissioning or encouraging education initiatives designed to improve the media literacy of members of the public. This will ensure Ofcom is taking action to directly support users to make safer choices online and make the most of all the internet has to offer, alongside the wider draft Bill which ensures online service providers take action to keep users safe. Alongside this, the Government has recently published the Online Media Literacy Strategy. This sets out our vision for supporting the empowerment of users with the skills and knowledge they need to make safe and informed choices online. Accompanying the Strategy we have published the first annual Online Media Literacy Action Plan which announced a series of Government-led initiatives to bring the Strategy to life. This includes establishing a Media Literacy Taskforce, funding a Train-the-Trainer programme for teachers and carers, and creating an online portal to support users to access media literacy resources. We have committed to publishing an annual Action Plan each year for at least the next three Financial Years.

82. Currently, it is difficult for users of many sites to manage their own and their children's safety online, as there is often a lack of transparency about how harmful information is dealt with and what is permitted. The approach that the Bill takes to legal but harmful content also supports user agency, by requiring platforms to make clear what types of harmful content are permitted on their sites and what action the platform will take if that content is found. This means that adults are able to make informed decisions about the types of content that they are prepared to encounter, and which sites they would prefer to avoid as a result.

THE ROLE OF OFCOM

Is Ofcom suitable for and capable of undertaking the role proposed for it in the draft Bill?

83. Ofcom has demonstrated its ability to deliver a diverse portfolio and take on new challenges. It is an experienced and established regulator, delivering complex high profile remits across broadcasting, telecoms, postal services and spectrum. However, the draft Bill sets out challenging and ambitious proposals for regulating an area whose scale and reach simply did not exist ten or even five years ago. Any regulator in this space would need to anticipate the changing landscape and build effective technical capabilities to regulate online harms. We are working closely together with Ofcom to support it in building the full range of necessary capabilities, including technical expertise, and to ensure it has the resources it needs.

84. The technological revolution of traditional industries has meant that digital and online services have increasingly become part of Ofcom's existing remit. It is further strengthening its digital capabilities through recruitment of experts from the private

sector. Ofcom already regulates video on demand services, and has experience in preventing children accessing inappropriate content.

85. Ofcom is experienced in regulating in a risk-based and proportionate way. This includes online services arising from its duties as the regulator for UK-established Video Sharing Platforms (VSPs). The VSP regime has allowed Ofcom to test regulatory processes ahead of online safety regulation coming into force. The intention is that the VSP regime will be superseded by the new regulatory framework.

86. Ofcom has strong existing relationships with other regulators, such as the Information Commissioner's Office, the Competition and Markets Authority and the Financial Conduct Authority. These bodies have recently formed a Digital Regulation Cooperation Forum which will allow them to work closely together and coordinate regulation of various aspects of the digital environment.

87. We are working with Ofcom to ensure it is able to build its expertise in relevant fields relating to national security and public safety issues that are covered by the Online Safety Bill, including online terrorism and CSEA. This includes building Ofcom's relationship with law enforcement and other relevant Government bodies.

Are Ofcom's powers under the Bill proportionate, whilst remaining sufficient to allow it to carry out its regulatory role? Does Ofcom have sufficient resources to support these powers?

88. Ofcom has a suite of powers under the Bill in order that it can fulfil its functions in regulating the new regime, including broad information gathering powers and robust enforcement powers. Where Ofcom identifies a breach of the duties, it has the power to impose substantial financial penalties, require companies to make improvements and/or pursue business disruption measures (including restricting access to non-compliant services). Ofcom will be required to exercise its statutory powers transparently and proportionately. Furthermore, Ofcom will need to apply to the Courts for business disruption orders, ensuring there is judicial oversight of these sanctions. We expect these to only be used in the most serious cases of user harm.

89. The government has committed to ensuring that Ofcom has the necessary resources it needs to set up the Online Safety regime and carry out its online safety functions effectively. Ofcom has drawn on its experience as an independent regulator to understand the skills and infrastructure necessary to build its capability as a regulator in the evolving digital space.

How will Ofcom interact with the police in relation to illegal content, and do the police have the necessary resources (including knowledge and skills) for enforcement online?

90. Ofcom will need to build strong working relationships with law enforcement to deliver a coherent approach to tackling online harms, including how their responsibility to regulate systems and processes interacts with law enforcement responsibilities to investigate illegal activity.

91. To support this cooperation, we have set up introductory meetings between Ofcom and law enforcement partners to help build understanding of roles and responsibilities, to share lessons on engaging with online platforms, and to share information on safety technologies that support the effective detection and removal of CSEA or terrorism online.

92. We will facilitate continued information exchanges between law enforcement and Ofcom on the nature and scale of online harms and support the development of information sharing agreements and memoranda of understanding on future working relationships.

93. On the question of police powers and resources, the Investigatory Powers Act 2016 (IPA) gives law enforcement powers to investigate illegal activity by requesting access to communications data i.e. the metadata associated with specific communications and the people or things responsible for them, but not the content. Powers under this act are available for any illegal activity online, because the legislation sets out that any offence which has the sending of a communication 'as an integral part' of that offence will surpass the "serious crime" threshold imposed. Additionally, law enforcement agencies have a power under Schedule 1 to the Police and Criminal Evidence Act 1984 (PACE) to apply to a judge for a production order for access to stored electronic data held by service providers.

94. There is also robust legislation in place to deal with internet trolls, cyber-stalking and harassment and perpetrators of grossly offensive, obscene or menacing behaviour. However, we recognise the complexities in adapting our approach against an ever-changing technological landscape. To ensure the criminal law is fit for purpose to deal with harmful communications online the Government has asked the Law Commission to review existing legislation on abusive and harmful communications. The Law Commission has now published its final report putting forward recommendations for reform. We will carefully consider bringing the Law Commission's final recommendations into law, where it is necessary and appropriate to do so. In addition, the Law Commission is undertaking a separate review sponsored by the Home Office, which is considering the adequacy and parity of protection offered by the law relating to hate crime. The Law Commission has consulted on their proposals and aims to publish a final report later this year.

95. The Government has invested in specialist investigation teams at regional and national level to provide the relevant knowledge, skills and capabilities for enforcement online:
    a. To improve the police response to victims of online hate crime we are funding a Police Online Hate Crime Hub, based in Greater Manchester Police but working nationally, which offers support and subject matter expertise.
    b. The Social Media Hub was established within the Metropolitan Police Service in June 2019, transforming the current capability and extending its reach to other forces. It brings together a dedicated team of police officers and staff to take action against online material, which includes making referrals to social media companies so illegal and harmful content can be taken down.

c. In 2010, we set up the Counter Terrorism Internet Referral Unit (CTIRU). The CTIRU identifies, assesses and refers online content that is in breach of UK terrorism legislation to tech companies for removal, in accordance with platforms' terms and conditions. To date, over 314,500 individual pieces of terrorist content referred by CTIRU have been removed by companies and the Unit also informed the design of the EU Internet Referral Unit based at Europol.
d. We have also invested in building the National Crime Agency's dark web capabilities to tackle the threat of child sexual abuse.

Are there systems in place to promote transparency, accountability, and independence of the independent regulator? How much influence will a) Parliament and b) The Secretary of State have on Ofcom, and is this appropriate?

96. We recognise the importance of an independent regulator for online safety. Ofcom's founding legislation already provides it with a high degree of independence. It is operationally independent from government with the statutory provisions to manage its own affairs. The draft Bill clearly sets out the scope of the regime and the remit of the regulator.

97. Ofcom, as the independent regulator, will lay its annual report and accounts before Parliament and be subject to Select Committee scrutiny. This will include the chair and senior managers appearing before Select Committees as well as pre-appointment scrutiny for the chair by the Department for Digital, Culture, Media and Sport Select Committee. This is in line with Ofcom's current arrangements.

98. Parliament will also have a role in approving a number of aspects of the regulatory framework through its scrutiny of secondary legislation.This will include the priority categories for harms and Ofcom's codes of practice. In addition the Secretary of State for Digital, Culture, Media and Sport will undertake a review of the effectiveness of the regime 2-5 years after entry into force, producing a report which will then be laid in Parliament. Parliament will have an opportunity to debate the findings of the report.

99. In some areas, the government will maintain appropriate levers to ensure the policy intent of the regulatory framework is maintained. These levers include:
    a. The ability for the Secretary of State to issue guidance, laid in Parliament, to Ofcom to provide further detail on specific elements of legislation. Ofcom will be consulted before guidance is issued or revised, and will then pay due regard to it.
    b. A provision for the Secretary of State to direct Ofcom to modify a code of practice that they have submitted, for certain specific reasons. It is important that there are suitable, transparent checks and balances to ensure that the implementation of the regime by the independent regulator delivers the policy intent that will be decided by democratically elected parliament.
    c. A power for the Secretary of State to issue a Statement of Strategic Priorities relating to online safety matters. The main purpose of such a statement would be to cater for changes in the digital and regulatory landscape. This power will

be similar to the Secretary of State's existing power in relation to telecommunications, management of the radio spectrum, and postal services.

Does the draft Bill make appropriate provisions for the relationship between Ofcom and Parliament? Is the status given to the Codes of Practice and minimum standards required under the draft Bill and are the provisions for scrutiny of these appropriate?

100. The draft Bill maintains Ofcom's existing accountability arrangements with Parliament. We consider these to be appropriate for online safety regulation.

101. Online safety legislation needs to cater for the huge variety of service providers in the sector in a proportionate way. The codes of practice will set out steps companies can take to fulfil their safety duties, providing a straightforward route to compliance for companies that want that, including very small companies. The sector is also exceptionally dynamic and innovative, and it is vital that companies should have the flexibility to take a different approach to carrying out their obligations. Companies that chose an alternative approach will need to be able to show the regulator that they have complied with the safety duties in the Bill.

102. The codes will be primarily technical and operational in nature. They will be prepared within the parameters established by the Bill, including being subject to an extensive consultation process. Laying the completed codes in Parliament under the negative procedure is therefore an appropriate level of Parliamentary scrutiny.

Are the media literacy duties given to Ofcom in the draft Bill sufficient?

103. Under Section 11 of the Communications Act 2003, Ofcom has an existing statutory duty to promote media literacy. This is a broad duty that charges Ofcom with a range of activities to promote media literacy with regard to electronic media, which includes communications occuring online.

104. The draft Bill clarifies this duty by amending the Communications Act to specify particular activities Ofcom should undertake as part of their duty. This includes:

a. carrying out, commissioning or encouraging education initiatives designed to improve the media literacy of members of the public;
b. preparing, keeping under review, and publishing guidance about the evaluation of media literacy initiatives;
c. carrying out research into media literacy; and
d. providing a clear definition of media literacy which provides Ofcom with context for carrying out the duty.

105. These specifications support wider policy ambitions to support organisations to improve evaluation practices across the sector; create a greater evidence base of the effectiveness of media literacy interventions through research and improved

evaluation; and to ensure all citizens have access to age and ability appropriate media literacy provisions and support. These ambitions have been informed by extensive research and stakeholder engagement, and are reflected as core challenges within the DCMS Online Media Literacy Strategy.

CONCLUSION

DCMS and the Home Office welcome the interest of the Joint Pre-Legislative Scrutiny Committee on the Draft Online Safety Bill and the DCMS Sub-committee on Online Harms and Disinformation in the draft Bill and its underpinning policy. We look forward to working with the Committees as they progress their work in this important area.