Government response to the House of Lords Communications Committee's report on Freedom of Expression in the Digital Age

Department for Digital, Culture, Media and Sport, October 2021

Introduction

1. The government welcomes this report and is grateful for the Committee's comprehensive inquiry into freedom of expression in the digital age. We are committed to maintaining a free, open and secure internet, in line with our democratic values.

2. The draft Online Safety Bill has been designed to deliver flexible and proportionate risk-based regulation. It seeks to tackle illegal content, protect children and empower users, while protecting the right to freedom of expression online. The draft Bill is currently subject to pre-legislative scrutiny, by a joint committee, due to report by 10 December. We will then introduce legislation when parliamentary time allows.

3. As the Bill undergoes pre-legislative scrutiny, the government will ensure that the legislation delivers on our commitments to protect freedom of expression online, while increasing user safety. The government's response provides further detail on how provisions in the Bill will protect free speech, responding to some specific concerns raised by the Committee.

4. The Online Safety Bill is one part of the government's strategy to increase user safety and protect pluralism online. This response therefore provides further information on how our Media Literacy Strategy and Safety by Design guidance will empower users online and support companies to build safety into their platform design.

5. The government agrees that competition is key to unlocking the full potential of the digital economy, and our proposed reforms will drive more vibrant digital markets, drive innovation and increase productivity. The government launched its consultation on the pro-competition regime for digital markets on 20 July and we will legislate to place this on a statutory footing as soon as parliamentary time allows. We note the Committee's views about the links between competition and free expression. As part of our engagement on the proposals, we are inviting views on the benefits and risks of giving the Digital Markets Unit powers to engage, in specific circumstances, with wider policy issues that interact with competition in digital markets.

Regulating content

6. **Recommendation 1 - The definition of 'content of democratic importance' in the draft Bill is too narrow. It should be expanded to ensure that contributions to all political debates—not only those debates which are about, or initiated by, politicians and political parties, and about policy, rather than social change—would be covered. The protections**

should also be extended to cover the content of platforms' terms and conditions, in addition to the "systems and processes" with which they apply them. (Paragraph 80)

7. **Government response:** The government agrees that the definition of 'content of democratic importance' must be broadly defined. The current definition in the draft Bill covers all political debates, including where these are advanced by grassroots campaigns and smaller parties. However, this definition does not afford protection to content that is designed to undermine democratic processes, such as harmful disinformation designed to damage the integrity of elections. Existing duties in the draft Bill requiring companies to protect democratic content extend to how they set their terms of service, not just the systems and processes with which they apply them.

8. The provisions in the draft Bill require providers of Category 1 services, those with the largest audiences and a range of high-risk features, to protect content of democratic importance, rather than to protect specific actors. This means that companies must have clear systems in place to protect content that is intended to contribute to democratic political debate in the United Kingdom, whether the creator of that content is a government minister or an individual political campaigner.

9. Clause 13(4) of the draft Bill requires platforms to specify in their terms of service their policies and processes to protect content of democratic importance. While platforms will have some discretion about what these policies are, they will need to balance the importance of protecting democratic content with their safety duties, and will still be able to remove content that is prohibited by their terms of service. For example, platforms will need to consider whether the public interest in seeing some types of content outweighs the potential harm it could cause, or vice versa. Clause 13(5) requires platforms to enforce these policies consistently across all content moderation.

10. **Recommendation 2 - We are concerned that platforms' approaches to misinformation have stifled legitimate debate, including between experts. Platforms should not seek to be arbiters of truth. Posts should only be removed in exceptional circumstances. (Paragraph 81)**

11. **Government response:** The government agrees that platforms should not seek to be arbiters of truth. The new regulatory framework will increase oversight of how the major platforms moderate content and prevent them from arbitrarily removing controversial content. Where harmful misinformation and disinformation does not cross the criminal threshold, the biggest platforms (Category 1 services) will be required to set out what is and is not acceptable on their services, and enforce the rules consistently. If platforms choose to allow harmful content to be shared on their services, they should consider other steps to mitigate the risk of harm to users, such as not amplifying such content through recommendation algorithms or applying labels warning users about the potential harm.

12. The Bill will hold platforms to account for the consistent enforcement of their terms of service. Clause 11(2) requires providers of Category 1 services to set out what harmful content, including misinformation and disinformation, is and is not acceptable in their terms of service. Clause 11(3) requires them to apply those terms of service consistently so that they do not remove content if it is not prohibited in their terms of service. This will ensure greater transparency about companies' policies, prevent the arbitrary removal of controversial content, and enable users to make informed decisions about the platforms they use.

13. Platforms must also consider and introduce safeguards for freedom of expression when setting their safety policies. Providers of Category 1 services will have to go further and assess their impact on free expression when adopting safety policies, and demonstrate they have taken steps to mitigate this impact. As set out above, these platforms will also be required to protect content of democratic importance.

14. **Recommendation 3 - The duty of care approach should inform a flexible framework for digital regulation, guided by underlying principles, including freedom of expression, which is able to adapt to the rapidly developing digital world while setting clear expectations for platforms. We discuss how this can be achieved—including the necessary parliamentary scrutiny and co-operation between regulators—in our subsequent conclusions and recommendations. (Paragraph 96)**

15. **Government response:** The government is committed to a flexible and proportionate regulatory approach, as set out in the government's Plan for Digital Regulation. The Plan for Digital Regulation describes new principles for how we will design and implement regulation so we actively promote innovation, achieve forward-looking and coherent outcomes, and exploit opportunities and address challenges in the international arena. It also sets out some practical steps the government is taking to embed this approach - including exploring opportunities to enhance coordination between regulators.

16. The draft Online Safety Bill is a key part of this overall approach and provides a proportionate and flexible framework to make service providers take more responsibility for the safety of their users and for upholding their users' rights. Codes of practice will set out steps relating to companies' processes for upholding freedom of expression and improving user safety when introducing content moderation or other online safety measures.

17. **Conclusion 1 - We support the Law Commission's aim of reforming communications offences. Although we heard compelling concerns about the appropriateness for social media of criminalising sending a communication which the defendant knew or should have known was likely to harm a likely audience, the Law Commission has now revised its proposal to require intent to harm —providing a clearer standard. However, we are concerned about the ability of social media platforms—in complying with their duties**

under the draft Online Safety Bill—to identify and remove content covered by the offence without also removing legal content. (Paragraph 111)

18. **Government response:** The government is carefully considering the Law Commission's recommendations, set out in its final report for its 'Harmful Online Communications review'. The draft Bill includes strong safeguards for freedom of expression which will minimise the risk of platforms removing legal content to comply with their new responsibilities.

19. If the government accepts and enacts the Law Commission's recommendations, relevant content would fall into the 'illegal content' category of the online harms framework. This means all companies in scope would need to address this material on their services, and comply with the requirements set out in the legislation in the same way that they would for any other illegal material, as defined in clause 41.

20. The approach to illegal content includes safeguards against over removal of legal content. Platforms will need to take action where they have reasonable grounds to believe that content amounts to a relevant offence. They will need to ensure their content moderation systems are able to decide whether something meets that test. However, platforms will not be penalised if they make a wrong call on whether particular pieces of content are illegal, so long as they have put appropriate systems and processes in place. When identifying illegal content, companies will be able to draw on Ofcom's codes of practice and any supplementary guidance.

21. Clause 12(2) also requires that companies have regard to the importance of protecting users' right to freedom of expression within the law when fulfilling their duties. Companies will therefore need to consider and implement safeguards for freedom of expression when fulfilling their duties, including when designing systems to identify and remove illegal content. Furthermore, providers of Category 1 services will have a duty to carry out an assessment of the impact that safety policies would have on protecting users' rights to freedom of expression and must set out any positive steps taken to secure users' rights to expression. These duties will reduce the risk that platforms over-remove content.

22. **Conclusion 2 - Police face many challenges, including from the scale of online content, anonymity, and the dark web. We are concerned that they do not have sufficient resources they need to enforce the law online. It is essential that the police can bring criminals to justice. The draft Online Safety Bill cannot be the only answer to the problem of illegal content. The government should ensure that existing laws are properly enforced and explore mechanisms for platforms to fund this. (Paragraph 123)**

23. **Government response:** The Online Safety Bill is not designed to substitute the work of law enforcement. Its focus is on requiring companies to mitigate the risk that services are used for criminal activity. The criminal justice system will continue to bring criminals to justice.

24. The Investigatory Powers Act 2016 (IPA) gives law enforcement powers to investigate illegal activity by requesting access to communications data. 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 obtain access to stored communications data held by service providers.

25. 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.

26. The government has invested in specialist investigation teams at regional and national level to provide the relevant knowledge, skills and capabilities for enforcement online:

- 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.

- 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 platforms so illegal and harmful content can be taken down.

- 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 of service. 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.

- We have also invested in building the National Crime Agency's dark web capabilities to tackle the threat of child sexual abuse.

27. **Recommendation 4 - The Government should require category 1 platforms to preserve deleted posts for a fixed period. Ofcom should also have the right to impose this requirement on category 2 platforms where appropriate. (Paragraph 124)**

28. **Government response:** The government does not agree that it would be appropriate to require providers of Category 1 services to preserve deleted posts for a fixed period.

29. Data retention for law enforcement purposes is already strictly regulated. The Investigatory Powers Act 2016 (IPA) provides the legislative framework to govern the use and oversight of investigatory powers in the UK. The default position is that no telecommunications operator is required to retain any data under the Act. Companies based in the UK have no legal obligation or right to retain content data unless required for business purposes. Where companies choose to retain content data for business purposes, law enforcement and the intelligence agencies may obtain this in limited circumstances under the IPA.

30. The IPA allows the Secretary of State to require certain companies to retain communications data for a maximum of 12 months, by giving them a retention notice. This must be necessary and proportionate, and for one or more statutory purposes including national security and the prevention and detection of crime. Communications data is the 'who, when, where and how' of a communication; such as username, IP address and some types of location data. Communications data is retained under the IPA for the hypothetical scenario that it may be relevant in a future crime. The majority of the retained data will never be accessed by law enforcement or the intelligence agencies, and strict safeguards govern data access.

31. Having consulted with law enforcement and other relevant parties, we do not consider that there would be a significant operational benefit in introducing a new requirement for companies to preserve posts. As such we do not intend to further legislate on this via the Online Safety Bill. We will continue to keep this under review, particularly in relation to the retention of child sexual exploitation and abuse content, where the government plans to introduce a requirement on companies to report this type of content to a relevant body.

32. **Recommendation 5 - In implementing clause 9(3)(d) Ofcom should set strict timeframes within which platforms must remove content which is clearly illegal. (Paragraph 132)**

33. **Government response:** Timeframes for the removal of illegal content are likely to be arbitrary and could have a negative impact on freedom of expression by incentivising over removal of content, without proper review by companies, in order to avoid penalties. We therefore do not agree that it would be appropriate to include this within the Bill.

34. The approach to illegal content within the Bill will require platforms to take a risk-based and proportionate approach to content removal, minimising the length of time for which priority illegal content is present. It focuses on ensuring companies have effective systems in place to identify and remove illegal content, while minimising the risk of over removal of legal content to avoid the risk of penalties for failing to comply with arbitrary time frames. However, when a provider becomes aware of any illegal content on their platform, it must take steps to swiftly take down such content or become liable for its presence.

35. **Recommendation 6 - The Bill should make clear that a platform would not be compliant if its systems to remove illegal content either systematically fail to remove illegal content or**

systematically remove legal content. This would ensure that platforms do not have an incentive to remove legal content. (Paragraph 133)

36. **Government response:** The draft Bill makes clear that if platforms fail to fulfil either their safety duties or duties in relation to free expression, Ofcom can take enforcement action.

37. Clause 9(3) of the Bill imposes a duty on platforms to implement systems and processes so they swiftly take down illegal content where they are alerted to its presence. It also requires them to put systems and processes in place so that they minimise the presence and dissemination of priority illegal content. Where platforms fail to achieve these objectives, they can be held liable by the regulator.

38. As set out in our response to recommendation 1, clause 12(2) of the Bill imposes a duty on platforms to have regard to the importance of freedom of expression within the law when fulfilling their duties. Ofcom's codes of practice will set out steps that platforms can put in place to safeguard freedom of expression when fulfilling their illegal content duties which platforms must either follow or show that alternative steps they have taken meet the same objectives.

39. **Recommendation 7 - The Government should ensure that all pornographic websites are in scope of the online safety regime and held to the highest standards. (Paragraph 149)**

40. **Government response:** Protecting children from online pornography is a government priority. The online safety regime will capture video-sharing sites, forums and content shared via image or video search engines, and pornography on social media. All pornography sites which host user-generated content or facilitate online user interactions (including video and image sharing, commenting and live streaming) will be in scope of the Online Safety Bill.

41. 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.

42. 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. The DCMS Secretary of State will use the pre-legislative scrutiny process to explore whether further measures to protect children are required.

43. **Recommendation 8 - Since the Digital Economy Act, age recognition technology has advanced. Websites are now able to use biometric age estimation technology, databases, mobile phone records and algorithmic profiling, alongside the ID based verification tools envisaged at the time of the Digital Economy Act. Such technological advances suggest it has been a missed opportunity for the Government to make clear on the face of the draft**

Bill that websites hosting pornographic content will be blocked for children. Children deserve to enjoy the full benefits of being online and still be safe. (Paragraph 150)

44. **Government response:** The draft Bill sets out very clear requirements for companies to prevent children accessing harmful content, such as online pornography. Companies that are likely to be accessed by children will need to use a range of age assurance technologies to comply with the new requirements and prevent children's access to such content.

45. For user-to-user services, clause 10 of the draft Bill sets out that providers must "*prevent children of any age from encountering, by means of the service, primary priority content that is harmful to children*". For search services, where children are likely to access their service, providers will be required to conduct a child safety risk assessment and take proportionate steps to minimise the risk of children encountering harmful content, such as online pornography, in or via their search results (clause 22).

46. Primary priority content will be set out in secondary legislation. This will be subject to the parliamentary process, however the December Full Government Response noted that pornography was a likely priority harm to children.

47. We expect Ofcom to take a robust approach to sites that pose the highest risk of harm to children, including sites hosting online pornography. This may include recommending the use of age verification technologies via codes of practice. Companies would need to put in place these technologies or demonstrate that the approach they are taking delivers the same level of protection for children, or face enforcement action by the regulator.

48. The Online Safety Bill has been designed to respond to the rapidly changing technological landscape. It takes a technology neutral approach, which future-proofs it and allows it to remain relevant despite changes in technology and online harms. It is important that there are trusted solutions available to support the legislation. The government is working with the safety technology and age assurance sector to put in place the right conditions for the market to develop innovative, secure and effective solutions in advance of legislation. This includes supporting the development of technical standards. The government is also engaging actively with companies in scope of the legislation to benchmark their current efforts on age assurance, set expectations and monitor their efforts for improvements. The previous Secretary of State wrote to popular social media platforms earlier this year, highlighting their failure to adequately enforce their minimum age requirements and asking them to detail how they intend to improve their measures.

49. **Recommendation 9 - If a type of content is seriously harmful, it should be defined and criminalised through primary legislation. It would be more effective—and more consistent with the value which has historically been attached to freedom of expression in the UK—to address content which is legal but some may find distressing through strong**

regulation of the design of platforms, digital citizenship education, and competition regulation. We discuss these in Chapters 3 and 4. (Paragraph 182)

50. **Government response:** The government's approach to harmful content accessed by adults that falls below the criminal threshold has been designed to protect freedom of expression and will not require companies to remove legal content. The Bill will increase transparency around companies' moderation processes, and ensure they are held to account for consistent enforcement of their terms of service.

51. The approach to harmful content accessed by adults is set out in detail in our response to recommendation 2. Category 1 services will need to set out clearly in their terms of service whether legal content that poses a risk of significant harm to adult users is allowed on their platform and how it will be treated if it does appear. The government will set categories of priority harmful content that companies must address in their terms of service, however companies will be free to determine their own policies for how they treat such content, so long as these are clearly understandable to users. Companies will need to assess how their design choices may pose a risk of harm to their users, and make clear in their terms of service how their design choices enable them to enforce their terms of service.

52. Companies will then need to enforce their terms of service consistently, or face enforcement action. Users will be able to appeal if they believe their content has been removed or down ranked in violation of a company's policies. This will mean that companies will no longer be able to arbitrarily remove content, including where it expresses controversial viewpoints. The approach will 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.

53. Our responses to recommendations 21-25 set out further detail on the work the government is doing to increase digital citizenship, media literacy and competition in digital markets. Work on digital citizenship is an important part in our strategy to address harms resulting from legal content, while the pro-competition regime for digital markets has the potential to support greater plurality and user choice in digital services.

54. **Recommendation 10 - If the Government does not accept our recommendation on an alternative approach to clause 11, it should improve the draft Bill in the following ways:**

- **The draft Bill provides two mechanisms by which content can be identified as harmful. The first is if a platform determines that it is of a type which the platform has, in its latest risk assessment, identified as posing a material risk of a significant adverse physical or psychological impact on an adult of ordinary sensibilities. The second is if it corresponds to a 'priority category' of content which the Secretary of State has, through regulations, deemed "harmful to adults". The latter mechanism should be removed from the draft Bill. It is superfluous and sets an unreasonably low threshold for harms.**

55. **Government Response:** The two mechanisms for companies to identify legal content have been designed to give certainty to businesses on the harms they must address, whilst ensuring the legislation remains agile and flexible to emerging harms and risks.

56. The power for the Secretary of State to designate priority harms will provide businesses with a list of the most serious and prevalent types of harmful content appearing on Category 1 services. It ensures that companies take a standardised approach to assessing the risk of these priority harms on their services and requires them to address these in their terms of service. This is critical for ensuring users are able to make informed choices about the platforms they use (as set out above).

57. The Secretary of State must consult Ofcom before determining the list of priority offences and Ofcom will provide advice on the prevalence and impact of harmful content. 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. Nevertheless, the requirement on companies to assess for other types of harm will ensure that companies swiftly identify and address harmful content, even where this is not on the priority list. It also ensures that companies address any platform-specific types of harmful content.

58. The regulations will be subject to appropriate parliamentary scrutiny.

- **The provisions of the draft Bill on content which is legal but may be harmful to adults should apply when the provider of the category 1 service has reasonable grounds to believe that content presents a significant risk to an adult's physical or mental health, such that it would have a substantial adverse effect on usual day-to-day activities. This is in line with the definition of serious distress in the Serious Crime Act 2015 and would provide greater clarity.**

59. **Government response:** Limiting the categories of content for which platforms have a duty to those that "would have a substantial adverse effect on usual day-to-day activities" would mean that companies could not be held to account for their treatment of content which causes real harm to users. For example, this definition would be unlikely to capture some forms of racist or extremist content.

60. The definition of content that is harmful to adults in clause 46 will ensure companies are transparent with users about their approach to a suitably broad range of content in their terms of service. It will also ensure that they can be held to account for inconsistent application of their terms of service, including the removal of content that is not clearly prohibited.

61. The test proposed by the Committee is used for the offence of controlling or coercive behaviour in a family or intimate relationship under section 76(4) of the Serious Crimes Act 2015. As set out above, platforms will not be required to remove legal content, but must set

clear terms of service for how they will deal with such content. It is therefore reasonable that companies are required to set terms of service for a broader range of content than that for which an individual may be held criminally liable but which does not have such a severe effect on individuals.

- **The reference in the draft Bill to indirect harm is particularly vague and could lead to the removal of legitimate content due to possible reactions to it by unreasonable people. It should be replaced with a reference to content which appears to be intended to encourage users to harm themselves or others.**
- **The Online Safety Bill should refer to the reasonable person of ordinary sensibilities.**
- **Under clause 46(6) of the draft Bill, where a particular adult is thought to be at risk they and their sensibilities replace the adult of ordinary sensibilities. This subjectivity should be removed.**

62. **Government response:** The definitions of content that is harmful to children (set out in clause 45) and adults (clause 46) have been designed to ensure companies have clarity about the types of content they must address.

    a. The requirement on companies to take action against content that may 'indirectly' harm an adult or child seeks to ensure companies respond to content that could cause a user to harm themselves or others. For example, content encouraging self-harm or extremist content.

    b. The reference to a person of 'ordinary sensibilities' seeks to ensure that companies are not required to respond to, for example, niche phobias. At the same time, it recognises that groups of individuals may possess characteristics that are not shared by the broader population, but result in them being targets of harmful content that could be foreseen or addressed by a provider. This could include, for example, harmful content relating to gender, faith, sexuality, race or disability.

    c. Clause 46(6) requires a provider of a service that has relevant knowledge about a person who is the subject of content to take that knowledge into account when assessing whether the content may be harmful to that person. Without this test, companies would not be required to address high impact harmful content which would only affect particular users. An example might be flashing images sent to someone with epilepsy, where the service provider is aware that they suffer from that condition.

63. The government will welcome views through the pre-legislative scrutiny period about the approach to this issue.

- **In the most serious cases, where a user has been banned from a category 1 platform, had their posts consistently removed or been forced off by abuse, they should have**

the right to appeal directly to an independent body, funded by but independent of the platforms, after exhausting the platform's own processes. (Paragraph 183)

64. **Government response:** Companies are best placed to respond to user complaints. The Bill will ensure that they put in place effective systems and processes to deal with user concerns, including those related to over removal of content and, on Category 1 services, content that is legal. Ofcom will oversee this requirement and will be able to take enforcement action if companies don't comply.

65. Category 1 companies will be required to have accessible and transparent systems and processes for users or other affected persons to easily report harmful content and activity, such as abusive content. Users must also be able to appeal if they believe that they or their content has been treated unfairly, such as when content has been removed even though it is not prohibited by the platform. Platforms will be required to take appropriate action in response to those complaints. This should ensure platforms address the concerns of users before they are forced off a platform due to abuse and protect against the consistent removal of content that is not prohibited by a company's terms of service.

66. Companies will be best able to consider the context of content, and then take action to remove it, sanction offending users, reverse wrongful content removal or change their processes and policies. Internal complaints mechanisms will also help companies understand their users' experiences, and provide them with valuable data to improve their systems and processes for tackling harm.

67. In addition, the super-complaints process will enable eligible organisations to submit evidence of systemic issues that are causing significant harm to users, members of the public or certain groups across one or more services, which Ofcom will review and respond to publicly. This could include evidence of widespread abuse as well as of over removal of content. Individuals can also seek redress through the courts in the event that a company has been negligent or is in breach of its contract with the individual. The new framework will not affect these rights and our regulatory model will provide evidence and set standards which may increase the effectiveness of individuals' existing legal remedies.

68. **Recommendation 11 - In Regulating in a Digital World, we recommended that a joint committee of both Houses of Parliament should be established to consider regulation of the digital environment. This committee would be responsible for scrutinising the adequacy of powers and resources in digital regulation. This would bring consistency and urgency to regulation. In addition, we found in this inquiry that there is a lack of scrutiny of delegated powers given to the Secretary of State and Ofcom. In relation to the latter, this raises serious concerns about democratic accountability. (Paragraph 184)**

69. **Recommendation 12 - We reiterate our recommendation that a joint committee of Parliament should be established to scrutinise the work of digital regulators. This joint**

committee should also scrutinise the independence of Ofcom and statutory instruments relating to digital regulation. (Paragraph 185)

70. **Government response:** As set out in the government's recent publication 'Reforming the Framework for Better Regulation: a consultation', while any changes to parliamentary business arrangements would be a matter for Parliament, we welcome views through that consultation on whether regulators should be more directly accountable to government and Parliament where they are given more flexibility in their governing legislation.

71. The new online harms regulatory framework will be a central part of the United Kingdom's digital regulatory landscape. Digital technologies are transforming the world at an unprecedented pace and impacting how we live and work. As set out in the Plan for Digital Regulation, the UK has the opportunity to write a rulebook for digital that has innovation at its heart, while keeping users safe and promoting our democratic values.

72. As new services, functions and harms emerge and platforms and users develop new ways to interact online, the online harms regulatory framework must be able to adapt to these changes. The delegated powers set out in the draft Bill ensure that the regime can evolve to continue to protect users, whilst adapting to the changing digital landscape and upholding democratic accountability.

73. The level of parliamentary oversight proposed for the exercising of each delegated power has been determined through assessment of the importance of the matter to be addressed and whether the delegated power amends primary legislation. Where the government has assessed that powers to amend primary legislation (so-called "Henry VIII powers") are desirable, it has ensured that each such power is limited to amending only specific provisions in the Bill. Without these powers the regulatory framework could quickly become inflexible and ineffective. All regulations made under Henry VIII powers in the Bill will be subject to the affirmative procedure. This will ensure that Parliament will be able to scrutinise any decision to amend primary legislation.

74. Ofcom, as an independent regulator, has a number of powers to supervise and enforce the regulatory framework. Ofcom's extensive experience as a communications regulator makes it best placed to develop the practical features and processes needed to regulate effectively and independently.

75. However, Parliament will have a continuing statutory role in determining Ofcom's priorities and aims. The Bill includes suitable and transparent checks and balances to ensure that Ofcom's implementation of the regulations delivers on the policy objectives decided by a democratically elected parliament. For example, the Codes of Practice must be approved by Parliament before entering into force.

76. Ofcom's independence from the government is clearly set out in statute, alongside its powers and duties. Ofcom is also accountable to Parliament, as stipulated by the Framework

Agreement between DCMS and Ofcom. While it would be within Parliament's powers to establish a new joint committee, Parliamentary scrutiny of Ofcom - alongside other digital regulators - should be conducted in such a way that does not question the nature of Ofcom's independence.

77. **Recommendation 13 - The Government should clearly define citizen journalism in the draft Bill. (Paragraph 196)**

78. **Government response:** We welcome your support for the protections in the draft Bill for journalistic content. The Bill will provide protections for all forms of journalism, including content produced by citizen journalists, without requiring further definition of this term.

79. The draft Bill confers a duty on providers of Category 1 services to safeguard journalistic content. This is defined as UK-linked content that is generated for the purposes of journalism. Platforms will therefore be required to ensure protections are applied to all content produced for the purposes of journalism, irrespective of the individual or organisation that generated the content. We therefore do not consider it necessary to include any additional definitions in order to capture specific types of journalism.

80. The draft Bill requires providers of Category 1 services to specify in their terms of service the method by which they identify content as being created for the purposes of journalism. In doing so, companies will be expected to consider the ordinary English meaning of journalism, the underlying purpose of protecting freedom of expression and information, and relevant case law. 'Journalism' should therefore be interpreted broadly and involve content produced by individuals, freelancers and others.

81. **Recommendation 14 - The online safety regime should require category 1 platforms to report annually on content they have been obliged to remove in other jurisdictions, whether by law or political authorities. This would allow UK users to know whether they are giving their custom to a platform which is complicit in censorship by authoritarian regimes. Users may wish to boycott platforms which value their profits more highly than human rights. The interventions we recommend in Chapter 4 to increase competition would make it easier for users to do so. (Paragraph 210)**

82. **Government response:** The objective of the Online Safety Bill is to protect users in the UK from harmful and illegal content and to protect their right to freedom of expression. The transparency reporting framework is one mechanism by which Ofcom can ensure that freedom of expression is being adequately and appropriately protected. Providers of Category 1 services will be required to produce transparency reports that include details of material removed by the platform and how a platform's operations will impact UK users. The DCMS Secretary of State will have the power to set additional thresholds to bring non-Category 1 services in scope for transparency reporting, if appropriate.

83. The legislation provides a high-level list setting out the types of information that companies could be required to include in their transparency reports. This list includes information about the steps that companies are taking to comply with the duties set out in Part 2 of the draft Bill, which include their duties about rights to freedom of expression and privacy. Ofcom will then specify the information that service providers will need to include in their transparency reports in the form of a notice.

84. Platforms may also be subject to legislative requirements by other countries which would require them to publish information about how their moderation policies function. Furthermore platforms may also include such information in the reports they produce on a voluntary basis.

85. However, it would not be appropriate to require companies to report on how their content moderation systems function in other jurisdictions where there is no link to UK users. Ofcom will not be responsible for overseeing platforms' compliance with legislative requirements in other jurisdictions.

Empowering users

86. **Recommendation 15 - Platforms must be held responsible for the effects of their design choices. The Government should replace the duties on category 1 platforms in relation to 'legal but harmful' content in clause 11 of the draft Online Safety Bill with a new design duty. Platforms would be obliged to demonstrate that they have taken proportionate steps to ensure that their design choices, such as reward mechanisms, choice architecture, and content curation algorithms, mitigate the risk of encouraging and amplifying uncivil content. This should apply both to new and existing services. The duty should include a requirement for platforms to share information about their design with accredited researchers and to put in place systems to share best practice with competitors. (Paragraph 241)**

87. **Recommendation 16 - Giving users more control over the content they are shown is crucial. This is more consistent with freedom of expression and the wide range of vulnerabilities and preferences users have than focusing on removing legal content. As part of the design duty we propose, the Online Safety Bill should require category 1 platforms to give users a comprehensive toolkit of settings, overseen by Ofcom, allowing users to decide what types of content they see and from whom. Platforms should be required to make these tools easy to find and use. The safest settings should always be the default. The toolkit should include fair and non-discriminatory access to third-party content curation tools. (Paragraph 242)**

88. **Recommendation 17 - Ofcom should allow category 2 platforms to opt in to the design duty on category 1 platforms, with a kitemark scheme to show users which meet this higher standard. (Paragraph 243)**

89. **Government response:** The government agrees that tech companies should be held to account where their design choices result in harm to users. The proposed regulatory framework will achieve this objective by requiring all companies in scope to consider the risks associated with their services, including risks arising from design choices or business models. Companies must then take steps to mitigate or effectively manage those risks.

90. In addition, the approach to legal but harmful content accessed by adults is designed to empower users to manage their own online safety. Category one companies must make clear what harmful content is acceptable on their service and enforce their rules consistently. If a category one company decides to tolerate some categories of harmful content, it may be appropriate to give users more control over the content they see and which other users they interact with to mitigate the risk of harm.

91. We are supportive of companies improving the ability of independent researchers to access their data, subject to appropriate safeguards. Ofcom will be required to produce a report on how, and to what extent, people carrying out independent research into online safety are currently able to obtain information from providers of regulated services to inform their research. After the publication of the report, Ofcom may prepare guidance about the issues dealt with by the report for providers of regulated services and people carrying out independent research into online safety. Our hope is that this will help companies and researchers overcome potential challenges associated with researcher access and will encourage safe and responsible sharing of data for research.

92. However, it is important that the regulatory framework is proportionate and risk-based. Imposing regulatory requirements in relation to 'uncivil content', which would be much broader than the current focus on harmful content, would be disproportionate.

93. **Recommendation 18 - Under the draft Online Safety Bill, as part of the user toolkit we propose, category 1 platforms should be required to allow users to opt out of seeing content from users who have not verified their identity. (Paragraph 255)**

94. **Government response:** The government recognises the concerns about anonymous abuse online. The new regulatory framework will address online abuse, including anonymous abuse, in a risk-based and proportionate manner that ensures bad actors cannot hide behind anonymous profiles to abuse others and evade accountability. We must do this in a way that ensures that those that rely on anonymity to speak truth to power or for their personal safety can do so, without being excluded from mainstream online debate.

95. The Online Safety Bill will require all companies to assess the risk of harms associated with functionalities that allow users to create anonymous and pseudonymous profiles, and to mitigate the risk of harm associated with this. The risk associated with anonymous profiles is likely to vary considerably depending on the nature of the service.

96. Ofcom will set out steps companies must take to mitigate the risk of harm, including by making their services safe by design. For example, companies will need to have effective systems in place to ensure that repeat offenders are not able to circumvent platform bans. If a company chooses to take an alternative approach, they will need to demonstrate that it is equally effective as the steps in the code.

97. **Recommendation 19 - Strong privacy standards should form part of the design duty we propose be added to the draft Online Safety Bill. (Paragraph 265)**

98. **Government response:** The draft Bill includes strong protections for privacy. It requires companies to have regard to the importance of protecting users from unwarranted infringements of privacy when carrying out their safety duties.

99. Providers of Category 1 services will have a duty to carry out an assessment of the impact that safety policies would have on protecting users' rights to privacy and must set out any positive steps taken to secure users' right to privacy. These provisions are intended to work alongside existing data protection legislation administered by the Information Commissioner's Office such that users can be assured that their privacy will be protected.

100. **Recommendation 20 - It is essential that regulators, including the Information Commissioner's Office, Ofcom, and the Competition and Markets Authority, co-operate to protect users' rights. (Paragraph 266)**

101. **Government response:** The government agrees that cooperation between regulators is key to delivering on our core objectives for digital regulation, including the protection of citizens' privacy and fundamental rights such as freedom of expression.

102. The Information Commissioner's Office, Ofcom and the Competition and Markets Authority (together with the Financial Conduct Authority) are already cooperating closely as part of the newly formed Digital Regulation Cooperation Forum. As set out in the Plan for Digital Regulation, the government is also considering whether further measures are needed to strengthen coordination at a statutory level.

103. **Recommendation 21 - Digital citizenship should be a central part of the Government's media literacy strategy, with proper funding. Digital citizenship education in schools should cover both digital literacy and conduct online, aimed at promoting civility and inclusion and how it can be practised online. This should feature across subjects such as Computing, PSHE and Citizenship Education. The latter is particularly crucial as it emphasises why good online behaviour is important for our society, our democracy and for the freedom of expression. (Paragraph 293)**

104. **Government response:** The new Online Media Literacy Strategy, launched in July 2021, sets out the government's approach to improving media literacy capabilities among internet users in England. This is accompanied by a Media Literacy Action Plan 2021/22 which sets

out eight initiatives that the government will fund or lead over the coming financial year. We will publish a new Action Plan each year until 2024.

105. The Strategy also outlines a Media Literacy Framework of best practice principles that set out the key skills and knowledge that are necessary for strong media literacy capabilities, and that the government believes should underpin media literacy initiatives. Each of these principles can be seen as a core component of effective digital citizenship, including Principle 4 of the Framework, which encourages users to understand that actions online have consequences offline, and use this understanding in their online interactions. Principle 5 encourages users to act kindly and responsibly online, understanding the impact this can have on others.

106. Media literacy skills and knowledge are included throughout the national curriculum in numerous places. This includes the computing and citizenship programmes of study; the statutory guidance for Relationships, Sex and Health Education (RSHE) which mandates teaching about online safety; and skills such as critical thinking which can be seen in subjects such as history, english and citizenship. We are committed to increasing the amount of media literacy activity taking place in schools. This year's Media Literacy Action Plan, for example, announces plans for the government to fund the roll-out of a media literacy training programme for teachers. This will support teachers to improve their own media literacy capabilities and feel more confident bringing those conversations into the classroom. At the same time, we recognise that the education system is just one route among many to improving media literacy in the UK, and our Strategy focuses on multiple pathways across the wider media literacy landscape to help educate and empower internet users.

107. **Recommendation 22 - The Government should commission Ofcom to research the motivations and consequences of online trolling and use this to inform a public information campaign highlighting the distress online abuse causes and encouraging users to be good bystanders. (Paragraph 294)**

108. **Government response:** As highlighted above, the government is committed to ensuring that users online are equipped with strong media literacy skills.

109. Ofcom has a duty to promote media literacy under the Communications Act 2003, within which it delivers a broad suite of research projects that provide insights into user behaviours online, and support the improvement of media literacy provisions. The draft Online Safety Bill details Ofcom's responsibilities, clarifying their existing duty. Ofcom already has the power to carry out this activity and is developing a new media literacy work plan in advance of the Bill's passage.

110. The Bill will also give Ofcom the power to conduct research into online harms. This will help Ofcom to develop a detailed understanding of the online harms landscape and will help build the existing evidence base about online harms. Ofcom will have the power to require

companies to provide information to support this research activity. Ofcom will have discretion over the specific research it undertakes, which will help ensure it is focussed where it is most needed.

111. **Recommendation 23 - We recommend that the strengthened duties in the draft Online Safety Bill on promotion of media literacy should include a duty on Ofcom to assist in co-ordinating digital citizenship education between civil society organisations and industry. (Paragraph 295)**

112. **Government response:** Through its duty to promote media literacy via the 2003 Communications Act, Ofcom has established the 'Making Sense of Media' programme of work to improve coordination within the UK's rich media literacy landscape.

113. Ofcom conducts robust research into media literacy and online safety trends that can be disseminated to the wider sector, coordinates relevant cross-sector stakeholders within their extensive network, and provides guidance on issues like improving standards of project evaluations.

114. As highlighted in response to recommendation 21, the Media Literacy Action Plan 2021/22 also sets out the government's commitment to enhancing media literacy and online safety coordination by setting up a Media Literacy Taskforce. The overarching goal of this Taskforce will be to take collective action in order to tackle 6 key challenges the media literacy sector faces, as outlined in the Strategy. In doing so, the Taskforce will convene key sector stakeholders and experts to ensure that user groups across society receive high quality education on media literacy and digital citizenship. The government will continue working closely with Ofcom on this initiative, to ensure best practice is shared in our respective approaches to tackling the key sector challenges.

115. **Recommendation 24 - Social media companies should increase the provision and prominence of digital education campaigns on their platforms. (Paragraph 296)**

116. **Government response:** The government welcomes the contributions made from the platforms in the digital education space, with several strong examples of digital citizenship programmes funded by the Tech sector. At the same time, we believe that these platforms must go further in this area.

117. Expanding on the point made in response to recommendation 21, the Online Media Literacy Strategy sets out a number of ways in which these platforms can scale-up their efforts. For example, the Media Literacy Framework sets out a series of actions that the platforms can take in order to address 5 media literacy principles, which ensure users can do the following:

    - Understand the risks of sharing personal data online, how that data can be used by others, and being able to protect their privacy online;

- Understand how the online environment operates and using this to inform decisions online;
- Understand how online content is generated and being able to critically analyse the content they consume;
- Understand that actions online have consequences offline, and using this understanding in their online interactions;
- Participate in online engagement and contribute to making the online environment positive, whilst understanding the risks of engaging with others.

118. Through the Strategic Sector Priorities laid out in the Strategy, the government also advocates for increased investment into both 'Literacy by Design' and in-person initiatives from the platforms. The former of these approaches encourages platforms to make design choices that will bolster their users' media literacy competencies, including by prompting them to use their critical thinking skills when posting, sharing, or otherwise engaging with online content. We are working closely with the platforms in order to ensure they play a proactive and impactful role in improving media literacy across society.

Promoting choice

119. **Recommendation 25 - The Government should introduce legislation to give statutory powers to the Digital Markets Unit during the current parliamentary session. This is if anything more important than the Online Safety Bill. Given the impact of competition on freedom of expression and privacy standards, the Digital Markets Unit should include human rights in its assessments of consumer welfare alongside economic harm. (Paragraph 319)**

120. **Government response:** The government launched its consultation on the pro-competition regime for digital markets on 20 July and we will legislate to place this on a statutory footing as soon as parliamentary time allows. Competition is key to unlocking the full potential of the digital economy, and our proposed reforms will drive more vibrant digital markets, drive innovation and increase productivity. This will result in better quality services for consumers, with greater choice and lower prices.

121. We note the Committee's recommendation that the Digital Market Unit should include human rights in its assessment of consumer welfare, alongside economic harm. We are currently conducting extensive stakeholder engagement during the consultation period (20 July - 1 October 2021) to capture diverse views on the design of the regime including the regime's overarching statutory objective. We are inviting views on the benefits and risks of giving the Digital Market Unit powers to engage, in specific circumstances, with wider policy issues that interact with competition in digital markets. We are also consulting on how the Digital Market Unit may coordinate with other digital regulators and regulatory regimes.

122. **Recommendation 26 - The Digital Markets Unit should make structural interventions to increase competition, including mandating interoperability. Where necessary, it should work with international partners—including to block mergers and acquisitions which would undermine competition. (Paragraph 333)**

123. **Government response:** The Digital Markets Unit will have powers to introduce interventions designed to open up digital markets to greater competition. These pro-competitive interventions aim to tackle the root causes of substantial and entrenched market power. They could include measures to overcome network effects and barriers to entry/expansion through mandating interoperability, third-party access to data or certain separation measures. They could also include measures that increase consumer control over data. We are consulting on the design and application of pro-competitive interventions, following an evidence based assessment.

124. Given the global reach of digital technologies, we recognise that it will be important for the Digital Market Unit within the Competition and Markets Authority to work closely with international partners to tackle competition issues in digital markets. Through our G7 Presidency this year, the G7 agreed to deepen international cooperation on digital competition. This includes work currently led by the Competition and Markets Authority to develop long term coordination and cooperation mechanisms between national competition authorities to better tackle competition concerns in global digital markets.

125. **Recommendation 27 - The Digital Markets Unit should make structural interventions to increase competition in the market, where necessary working with international partners. This should include forcing Google to share click-and-query data with rivals and preventing the company from paying to be the default search engine on mobile phones. (Paragraph 346)**

126. **Government response:** As noted above, the government agrees that the Digital Markets Unit should have the power to make structural and behavioural pro-competitive interventions to increase competition in digital markets. These remedies will be implemented in relation to firms who have been designated with strategic market status, and will be the result of an evidence-based investigation led by the Digital Markets Unit.

127. **Recommendation 28 - The Government should require Ofcom to give due consideration to—and report on the impact on—competition in its implementation of the regime. Ofcom should work closely with the Digital Markets Unit in this area. (Paragraph 358)**

128. **Government response:** We support the development of informal coordination mechanisms including the Digital Regulation Cooperation Forum. The Digital Market Unit will work closely with Ofcom on a wide variety of objectives, including digital competition. The government is consulting on a range of coordination mechanisms between the Digital Market Unit and

other digital regulators, including those with a statutory objective to promote competition (which includes Ofcom).

129. **Recommendation 29 - To avoid UK users losing access to these websites, the Government should introduce a third category for platforms which are based abroad and have very few UK users. This would include websites such as local newspapers and message boards for people with niche interests. We expect that Ofcom would set a threshold for the number of UK visitors per year to allow platforms to know whether they are in category 2 or 3. Although category 3 platforms would be held to the same safety standards as category 2 platforms, to reduce the regulatory burden on them category 3 platforms would have no duties proactively to prove compliance unless Ofcom notified the company—after completing its own risk assessment, or receiving complaints from users or a third-party—of further steps it should take in relation to illegal content or content which may be harmful to children. (Paragraph 360)**

130. **Government response:** We are confident that the draft Bill gives Ofcom the power to act where it needs to, without bringing into scope broad swathes of the internet which pose no real risk to people in the UK.

131. The legislation will apply to any service that is linked to the UK and is enabling harm to UK users. A service is linked to the UK if the service has a significant number of UK users, UK users form a target market for the content, if the content is likely to be of interest to UK users or if the service is capable of being used in the UK. Additionally, a service has links to the UK if there are grounds to believe that there is a material risk of harm to UK individuals arising from the service.

132. All companies with the relevant link to the UK that fit the other criteria in the Bill (e.g. being a user-to-user service or a search service) must comply with the duties established under the Bill, wherever they are based. This minimises the risk of regulatory loopholes for bad actors to exploit while avoiding placing onerous and unnecessary burdens on smaller platforms outside of the UK. Ofcom will therefore be able to take enforcement action against companies outside of the UK, if they are in scope.

133. Ofcom will take a risk-based, targeted and proportionate approach to oversight and enforcement. It will be firmly focused on protecting UK users and others in the UK who may be victims of online harm.

134. **Recommendation 30 - The Digital Markets Unit should make structural interventions to increase competition, including through separation remedies. (Paragraph 370)**

135. **Government response:** As noted above, the government agrees that the Digital Markets Unit should have the power to implement structural and behavioural remedies within SMS firms, including certain separation remedies. We are consulting on whether any particular

measures should be excluded from the Digital Markets Unit's toolkit, including ownership separation.

136. **Recommendation 31 - We reiterate our recommendation for a mandatory bargaining code to ensure fair negotiations between platforms and publishers. Google's and Facebook's voluntary initiatives to pay some publishers for some of the use of their content are welcome. However, such agreements reflect the fundamental imbalance of power between the two sides. As the Competition and Markets Authority has noted, publishers have little choice but to accept the terms they are offered. Only a mandatory bargaining code, with the possibility of independent arbitration, can ensure that publishers—particularly smaller and local publishers—get a fair deal. The code should also cover how platforms use and curate publishers' content. (Paragraph 389)**

137. **Government response:** The government is committed to defending the freedom of the press and enhancing the sustainability of journalism. The pro-competition regime's code of conduct represents just one aspect of our wider support for news publishers. In line with the codes proposed in the 2019 Cairncross Review, the pro-competition regime's code will improve competition and transparency and so make an important contribution to the sustainability of the press.

138. Beyond this, we have not ruled out any options regarding our support for the press sector, and we invite views through our consultation on what more might be done to address the unbalanced relationship between key platforms and news publishers. Our thinking will also be informed by the ongoing work of the Digital Markets Unit and Ofcom, as they look at how a code would govern the relationships between platforms and content providers such as news publishers, including to ensure they are as fair and reasonable as possible. We also continue to engage with other jurisdictions, including with the Australian government and the Australian Consumer and Competition Authority, to develop our understanding of the effect of their approach to this issue, and the reactions from both publishers and platforms.