House of Commons

Digital, Culture, Media and Sport Committee

The Draft Online Safety Bill and the legal but harmful debate: Government Response to the Committee's Eighth Report

Fifth Special Report of Session 2021–22

Ordered by the House of Commons to be printed 22 March 2022

HC 1221
Published on 24 March 2022
by authority of the House of Commons

The Digital, Culture, Media and Sport Committee

The Digital, Culture, Media and Sport Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Department for Digital, Culture, Media and Sport and its associated public bodies.

Current membership

Julian Knight MP (*Conservative, Solihull*) (Chair)

Kevin Brennan MP (*Labour, Cardiff West*)

Steve Brine MP (*Conservative, Winchester*)

Clive Efford MP (*Labour, Eltham*)

Julie Elliott MP (*Labour, Sunderland Central*)

Rt Hon Damian Green MP (*Conservative, Ashford*)

Dr Rupa Huq MP (*Labour, Ealing Central and Acton)*

Simon Jupp MP (*Conservative, East Devon*)

John Nicolson MP (*Scottish National Party, Ochil and South Perthshire*)

Jane Stevenson MP (*Conservative, Wolverhampton North East*)

Giles Watling MP (*Conservative, Clacton*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/dcmscom and in print by Order of the House.

Committee staff

The current staff of the Committee are Keely Bishop (Committee Operations Assistant), Andy Boyd (Committee Operations Manager), Joe Briggs (Committee Specialist), Laura Caccia (Second Clerk), Dr Conor Durham (Committee Specialist), Ollie Florence (Senior Media and Communications Officer), Lois Jeary (Committee Specialist), Dr Stephen McGinness (Clerk) and Billy Roberts (Media & Communications Officer).

Contacts

All correspondence should be addressed to the Clerk of the Digital, Culture, Media and Sport Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6188; the Committee's email address is dcmscom@parliament.uk.

You can follow the Committee on Twitter using @CommonsDCMS.

Fifth Special Report

The Digital, Culture, Media and Sport Committee published its Eighth Report of Session 2021–22, The Draft Online Safety Bill and the legal but harmful debate (HC 1039), on 24 January 2022. The Government Response was received on 17 March 2022 and is appended below.

Appendix: Government Response

Executive Summary

Objectives of the draft Online Safety Bill

1. The internet has transformed our relationships, working environments and exposure to the wider world. UK citizens now use the internet more than ever. Internet usage across all adult age groups increased by nearly 10% from 2009 to 20191.[1] However, unfortunately not all of the internet offers a positive experience for users. 62% of adult internet users reported having had at least one potentially harmful online experience in 2020 – worryingly this figure increases to over 80% for 12–15 year olds.[2] That is why we have made our commitment to develop legislation that will enable the UK to be the safest place in the world to go online, and the best place to grow and start a digital business.

2. The main priority for this legislation is to protect the safety of internet users. Under the new laws, in-scope platforms will need to:

a) **Tackle illegal content and activity** – There will be no safe space for criminal content online. Platforms will have to quickly remove illegal content such as terrorist or child sexual abuse and exploitation material, and will not be allowed to promote it via algorithms.

b) **Protect children** – The strongest protections in our new laws are for children and young people. They will be protected from harmful or inappropriate content such as grooming, bullying, pornography and the promotion of self-harm and eating disorders.

c) **Give adults greater control, while protecting freedom of expression:** This legislation will close the gap between what companies say they do, and what they actually do. Online content that is legal can still, in some cases, have a seriously damaging impact on adults, e.g. racist and misogynistic abuse or suicide and self-harm content which does not meet the criminal threshold. The largest and riskiest companies will need to set out clearly in terms and conditions what harmful material is allowed on their sites, and take effective action to enforce their terms and conditions. In doing this, the Bill will protect our core democratic rights – in particular the right to free expression, by increasing transparency about content moderation and ensuring users' can appeal arbitrary content and account removal.

1 Adults' Media use and Attitudes report' (2005–2019) – Ofcom
2 Internet users' experience of online harms – Ofcom and ICO (2020)

3. The new legislation will achieve these outcomes by giving Ofcom powers to oversee and enforce the regulatory framework. The framework will remain proportionate and risk-based, and we are committed to ensuring that the legislation is flexible, with provisions in place that are futureproofed and subject to ongoing scrutiny.

Summary of the Committee's recommendations and Government responses

4. The Government is grateful to the Committee for its report on the draft Bill. The breadth and depth of the inquiry and the range of evidence gathered underlines the importance of the Online Safety Bill.

5. The Committee made a number of recommendations about the draft Bill. The Government welcomes the report, which in many areas aligns with the Government's commitment to delivering groundbreaking legislation that makes the UK the safest place in the world to be online, while protecting freedom of expression. As a result, we are accepting eight of the Committee's recommendations. In some areas, we agree with the Committee's policy intent but intend to deliver it in a different way. There are some recommendations that we disagree with. In these instances, we have set out detailed rationale for the Government's position below. Further details are provided in the following chapters.

Key points in our response – Digital Markets and Digital advertising

6. We welcome the Committee's interest in the UK's framework for digital regulation, in particular the Government's work on online advertising and digital markets. The Committee asked the Government to update on its work on online advertising and digital markets. The Government set out its plans for a new pro-competition regime for digital markets in a public consultation in July 2021. The new regime will boost innovation and growth through tackling economic harms. We are carefully considering responses to the consultation and will publish our response soon. We will legislate as soon as parliamentary time allows.

7. We published the Online Advertising Programme consultation on 9 March. The consultation seeks responses within a 12-week period and we are likely to publish our response to these in the autumn. The Online Safety Bill will also take immediate action in tackling fraudulent advertising.

Safety duties

8. As stated above, the Bill's key objectives are to tackle illegal content and activity, protect children and give adults greater control, while protecting freedom of expression. We welcome the Committee's input on further clarifying and strengthening service providers' duties.

9. We agree with the Committee that illegal content should be subject to the most stringent measures. All services subject to the safety duties will be required to operate their services using systems and processes to proactively prevent users from encountering priority illegal content on their services. We also welcome the Committee's recommendation that the Bill

should contain more detail about the measures service providers can take to comply with their duties. We have added non-exhaustive, indicative categories of the types of measures that providers can take to fulfil their safety duties for illegal content, and protect children from harmful and age-inappropriate content, to the Bill.

Definitions of harm

10. We understand the Committee's view that the Bill should offer more clarity about the types of harms in scope of the Bill. We support the Committee's recommendation regarding the inclusion of priority offences and, on 7 February 2022, we announced that priority offences would be included on the face of the Bill. This change will allow the illegal content duties to be brought into force more quickly, and will provide greater clarity and certainty about the requirements under the online safety regime. This will result in earlier accountability for companies, which in turn will force rapid action against illegal harms. In addition, in-scope services subject to safety duties will still have to remove illegal content relating to criminal offences with individual victims that do not appear on the list of priority offences, where they become aware of the content.

11. We are also making changes to the definitions of content that is harmful to adults and content that is harmful to children. We have removed the requirement for companies to address non-priority content that is harmful to adults, to give Parliament full control over which legal content accessed by adults should be addressed by platforms. Priority content harmful to children and adults will be designated in secondary legislation, providing certainty to affected service providers. This will also ensure providers do not face pressure to address content beyond what is set out in law.

Designation of types of harm

12. We are clear that the Bill must be future-proofed and that Parliament should have a role in designating future harms. The draft Bill already set out that the Secretary of State will be able to designate categories of content that is harmful to adults and content that is harmful to children in secondary legislation. The Committee recommended that all designations of harmful content should be subject to the affirmative resolution procedure. We agree with the Committee, and have updated the Bill so that changes to the regulations to specify types of harm should be subject to the affirmative resolution procedure, as well as the initial regulations. The affirmative procedure will therefore apply to the designation of new types of harmful content in urgent cases. This will give Parliament a key role in determining future changes to the types of harms in scope of the regime and will provide greater certainty for service providers subject to the safety duties.

Transparency and information-gathering

13. Delivering greater transparency, trust and accountability is at the heart of the new regulatory framework. To support this the regulator will have a broad range of powers which will help to ensure it can access the information it needs to understand how companies are fulfilling their duties. We are satisfied that these powers will cover the examples of information put forward by the Committee and that Ofcom will be equipped to gather

the information it needs to effectively regulate the sector. We will also be bringing forward senior management liability for non-compliance with information requests, rather than including this in the Bill as a deferred power.

14. We welcome the Committee's recommendation that Ofcom should have a power to conduct auditing of a service's systems to assess how a platform's systems are working in practice and can confirm that such a power has been added to the Bill.

Enforcement

15. Ofcom can take enforcement action against providers of regulated services if they breach any of their duties under the Bill. Ofcom will consult and publish enforcement guidelines covering the new regime, which will provide more detail on how it intends to use its enforcement powers.

16. We are making improvements to Ofcom's Use of Technology notice power (now referred to as 'Notices to deal with terrorism content or CSEA content (or both)') in line with the Committee's feedback. We have amended the Bill to ensure that this power provides a robust response to the extremely concerning prevalence of CSEA online, while also ensuring there are built-in safeguards to ensure users' rights are upheld.

17. We are also mindful of the changes happening in how the internet functions. We want to ensure the regulator's powers are future-proofed as far as possible. As such, business disruption provisions have been drafted in outcome-focussed tech and actor-neutral terms. We are confident that we have future-proofed these provisions to cover future technological changes.

User redress

18. The Bill contains strong user redress provisions. The Committee recommended that the Government should provide further clarity about the provisions, including that the super-complaints mechanism does not override users' ability to access the courts. We are clear that none of these provisions, including the super-complaints mechanism, prejudice the right of individuals to access courts. The courts are an important way that users can seek redress where a company has breached its own terms of service. As such, we have included a provision in the Bill which requires all user-to-user services to make clear in their terms of service that users have a right to bring a claim for breach of contract in court when their content is removed or restricted in breach of the service provider's terms of service.

Parliamentary scrutiny

19. We agree that effective parliamentary oversight has an important role to play in this fast moving space. While we see considerable value in the two houses working together to provide consolidated scrutiny of digital regulation, we understand the concerns of the Committee about the establishment of a new permanent committee. The Government intends to work with Parliament to support scrutiny of the Online Safety Act in a way that utilises the skills and expertise in both Houses, but will not be supporting the establishment of a permanent Joint Committee on Digital Regulation.

Pre-legislative Scrutiny

DCMS Committee Recommendation – Pre Legislative Scrutiny (Para 3)

1. ***We are pleased that the Government listened to our calls for pre-legislative scrutiny and decided to publish the Online Safety Bill in draft. We also welcome the recent, comprehensive work by the Joint Committee on the Draft Online Safety Bill, the Treasury Committee and the Lords Communication and Digital Committee and anticipate upcoming Reports from the Petitions Committee (on online abuse) and others. It is also important to note that the online safety regime will form only one part of the UK's framework for digital regulation and we hope that the Government will take a similar, collegiate approach, such as giving time for pre-legislative scrutiny, in these areas. The Government should provide an update on its work on online advertising and digital markets in response to this Report and publish its responses to the consultations in each of these areas by the time it responds to us in two months' time.***

Government Response

Digital Markets

2. The Government set out its plans for a new pro-competition regime for digital markets in a public consultation in July 2021. The new regime will boost innovation and growth through tackling economic harms.

3. In November 2020, the Government committed to establishing a new regime. This followed the findings of the 2019 Furman Review into digital markets, and the CMA's 2020 market study into online platforms, which found a small number of dominant tech firms are stifling UK economic growth, imposing unnecessarily high costs on small businesses, and making UK families worse off.

4. The new pro-competition regime is designed to drive up competition and innovation and rebalance the relationship between dominant tech firms and the users who rely on their services.

5. At the heart of the regime is a code of conduct to govern the behaviour of big tech companies to help promote fair trading, open choices, trust and transparency. Additionally, 'pro-competitive interventions' will open up digital markets to greater competition by addressing the root causes of market power.

6. We are carefully considering the design of the new regime so that it does not create inconsistencies, gaps or overlaps with other parts of the regulatory landscape. This includes effective join-up between the new Digital Markets Unit and established regulators to ensure effective collaboration and clarity across the digital regulatory landscape.

7. We are carefully considering responses to the consultation and will publish our response soon. We will legislate as soon as parliamentary time allows.

Online Advertising

8. We published the Online Advertising Programme (OAP) consultation on 9 March. The OAP will consider holistically how online advertising is to be regulated, with the aim of fostering fair, accountable and ethical online advertising that works for citizens, businesses and society as a whole.

9. The Online Safety Bill will also take immediate action to tackle a specific type of harmful advertising. We recognise the urgent need for regulation that tackles fraudulent adverts, and are aware that some services in scope of the framework play a role in disseminating these adverts online. Therefore, the Online Safety Bill contains a new stand-alone duty on these platforms (Category 1 and 2A) to prevent the publication of fraudulent adverts on their services. The Online Safety Bill now, for the first time, places a duty of care on the largest platforms, to ensure that they protect their users from harmful, fraudulent adverts.

10. Following from this, the OAP will look at the whole ecosystem in order to capture all the players in the supply chain that have the power and capability to do more to combat fraudulent advertising. This includes intermediary businesses and/or services which connect buyers and sellers (e.g through programmatic trading), facilitate transactions, and leverage data to provide buyers with targeting options for online advertising. Demand Side Platforms (DSPs) and Supply Side Platforms (SSPs)—both of whom play a critical role in the delivery of some forms of online advertising—will fall under this definition.

11. The online advertising ecosystem is a complex one with many firms of varying sizes playing different roles in the market. We anticipate that the OAP will introduce systems and processes in order to improve transparency and accountability across the supply chain, taking a proportionate approach to ensure we address harm but do not stifle innovation or growth.

The duties of care

Summary

- This chapter focuses on the definition and designation process of the different types of harm the regulatory framework will tackle, and the way platforms' duties are set out in the Bill.
- The Government has been clear that the objectives of the duties of care are to tackle illegal content and activity, protect children and give adults greater control, while protecting freedom of expression.
- The Committee's recommendations in this area are focused on providing greater clarity and direction to companies about the types of harms that they must address and the steps they must take to tackle this content.
- Since publication of the draft Bill, we have developed the Bill further to:
  - add non-exhaustive, indicative types of measures that providers can take to fulfil their safety duties for illegal content and protecting children.

- include an exhaustive list of priority offences on the face of the Bill.
- make changes to better clarify the definitions of content that is harmful to adults and harmful to children.
- update the Bill so that changes to the regulations to specify types of harm should be subject to the affirmative resolution procedure.

DCMS Committee Recommendation – Illegal content (Para 10)

12. ***The Government should redraft the Online Safety Bill to state explicitly that the scope of the framework for addressing "illegal content", which should be subject to the most stringent moderation measures, specifically applies to existing criminal offences, rather than regulatory offences and civil or administrative wrongs.***

Government Response

13. We welcome the Committee's focus on the definition of illegal content in the draft Bill. The Government has always been clear that one of the main aims of the legislation is to require companies to take action to prevent the proliferation of criminal content and activity online.

14. We agree with the Committee that duties relating to illegal content should only apply to criminal offences. Our view is that the Bill already achieves this. The definition of illegal content within the Bill relates only to criminal offences, and these do not exist in civil or administrative law.

15. The Bill then makes clear that criminal offences that concern the infringement of intellectual property rights, as well as consumer protection legislation, are not covered, as that would lead to regulatory duplication.

16. The most stringent duties in the Bill will apply to the most serious criminal offences which can be committed online – these are the terrorism, CSEA and other priority offences set out in Schedule 7 to the Bill. Service providers subject to the safety duties will be required to operate their services using proportionate systems and processes to prevent users from encountering priority illegal content and activity on their services, and to remove it where it appears.

17. Service providers subject to the safety duties will also be required to have systems and processes in place to remove any other content that amounts to a criminal offence targeting an individual, when they become aware of it.

DCMS Committee Recommendation – Provisions to protect children (Para 12)

18. ***Though the Bill takes several welcome steps to address harms to children, such as duties to tackle child sexual exploitation and abuse (CSEA), we are concerned about the prevalence of content and activity that are seemingly not captured by the proposed regime. One example of such activity is breadcrumbing, where perpetrators deliberately subvert the thresholds of criminal activity and for content removal by a service provider. We recommend that the Government respond to our concerns about the risk of content***

and activity that falls below the threshold of outright criminal activity but nonetheless forms part of the sequence for online CSEA. One starting point should be to reframe the definition of illegal content to explicitly add the need to consider context as a factor, and include explicitly definitions of activity like breadcrumbing, on the face of the Bill.

Government Response

19. We share the Committee's concern about all forms of online child abuse, including 'breadcrumbing' or content that falls below the criminal threshold. Such activity and material is extremely harmful to victims and can be used to facilitate CSEA offending.

20. Some forms of contextual CSEA are captured by existing offences, and companies subject to the safety duties will therefore need to address this content as a result of the illegal content safety duties. This includes photoshopped images and sexualised content of children. To ensure as much contextual CSEA as possible is dealt with as illegal content, the Obscene Publications offence, which covers online communications about CSEA has now been added to the list of priority offences in the Bill for introduction.

21. Please also note that companies subject to the safety duties will need to implement systems and processes so that they can fulfil their duties for illegal content. Ofcom will recommend systems and processes and set out how they should be implemented in codes of practice. These are likely to include appropriate content moderation systems so platforms are able to take context into account when making decisions about how to treat content.

22. The regime will also address CSEA material which falls below a criminal threshold in the followings ways:

a) Under the regulatory framework, companies which are likely to be accessed by children will need to protect children from legal but harmful content, which presents a material risk of significant harm to an appreciable number of children. This could include content and activity that falls below the threshold of criminal activity but forms part of the sequence for online CSEA.

b) Equally, the Bill will oblige the largest and riskiest companies to be transparent and consistent about how they treat legal but harmful material when accessed by adults. Category 1 companies (high risk and high reach) will have to set out in their terms of service how they will address legal but harmful material, explaining how this responds to their risk assessments, and enforce those terms consistently and transparently.

c) Finally service providers subject to the duties will have a statutory duty to have effective and accessible reporting and redress mechanisms for users, and non-users who may be directly affected, so that they can report illegal content and activity. This will include victims of CSEA whose images have been shared online, including where they are not the users of that service, as well as parents or guardians wishing to report concerns on behalf of a child. Users and non-users directly affected will also be able to report content that is harmful to children to services likely to be accessed by a child and content that is harmful to adults to Category 1 services. They should expect to see platforms responding quickly

and effectively in response, which could include the removal of harmful images, sanctions against offending users, or changing their processes and policies to better protect their users.

23. Providers of services subject to the safety duties will also be required to report CSEA detected on their platforms (detected through automated monitoring systems, human review, user reports or other means) to the National Crime Agency. The requirement does not intend to duplicate reporting efforts, therefore a service provider may be exempt if it already reports elsewhere. Reports of CSEA must meet specified requirements set out in regulations to ensure service providers make high quality reports with the vital information needed by law enforcement to safeguard children, identify offenders, and prevent lifelong re-victimisation through the ongoing recirculation of illegal content.

DCMS Committee Recommendation – Content that is harmful to adults (Para 19)

24. ***Proposed amendments to the Draft Bill thus far have been a missed opportunity in making the broader definitions of harm compatible with international human rights law and address societal harms like Covid-19 disinformation. We reiterate our conclusion from a previous Report that doing so is not mutually exclusive. We recommend that the Government reframes the language around considerations for freedom of expression to incorporate a 'must balance' test so Ofcom can interrogate and assess whether providers have duly balanced their freedom of expression obligations with their decision making.***

Government Response

25. We agree with the Committee that the Bill must have strong protections for freedom of expression. We have designed the regulatory framework to balance protecting users' safety and protecting users' freedom of expression. Service providers subject to the safety duties and Ofcom have duties for freedom of expression, for which they can be held to account. These protections are in place of a 'must balance' test. A 'must balance' test suggests there is a clear line to be drawn regarding when legal content should be removed. This is in conflict with Government policy, which accepts that it would be inappropriate for the Government to require companies to remove legal content accessed by adults.

26. It also recognises that service providers, as private companies, have the right to remove legal content from their services. Preventing them from doing so, by requiring them to balance this against other priorities, could have perverse consequences. Therefore, companies subject to the safety duties must set clear terms of service for how they will treat such content, and ensure these are properly enforced. When setting these terms of service, those companies must consider their impact on freedom of expression.

27. Finally, if this test was overseen by Ofcom, this would delegate an inappropriate degree of power to a regulator to determine what legal content is permissible online, and how companies should treat this. It would effectively require Ofcom to decide what legal content companies could and could not remove.

DCMS Committee Recommendation – Content that is harmful to adults (Para 20)

28. ***We recommend that the Government also reframes the definitions of harmful content and relevant safety duties for content that is harmful to children and content that is harmful to adults, to apply to reasonably foreseeable harms identified in risk assessments, and explicitly add the need to consider context, the position and intentionality of the speaker, the susceptibility of the audience and the content's accuracy. These factors would bring the Bill into line with international human rights law and provide minimum standards against which a provider's actions, systems and processes to tackle harm, including automated or algorithmic content moderation, should be judged.***

Government Response

29. We agree that the approach to legal but harmful content needs to uphold users' rights online and provide clarity to businesses about what is expected of them. Rather than using the Committee's proposed reframing, we have made other changes that meet a similar objective whilst providing more clarity and not requiring the removal of legal content, which would have a negative impact on users' rights.

30. To address concerns about the approach to legal but harmful content, we have taken a number of steps. First, we have simplified the definition of harmful content. In the revised Bill, content is considered harmful if it presents a material risk of significant harm to an appreciable number of children/adults.

31. Secondly, for adults, we also are removing the requirement for Category 1 service providers to address non-priority harmful content (other than to report its presence on their services to Ofcom). Instead every category of content that is harmful to adults covered by companies' safety duties will be set out in secondary legislation. This change will make it clearer to Category 1 service providers which types of content they are required to address and give Parliament full oversight of what is defined as content that is harmful to adults. It will also strengthen protections for freedom of expression by reducing the risks of over-removal of legal content as a result of the safety duties. Category 1 service providers will continue to be required to report emerging types of harmful content to Ofcom.

32. Finally, for children, the Government is designating priority categories of content that is harmful to children in secondary legislation to ensure that companies subject to the child safety duties take a robust and consistent approach to protecting children from harms which have the most significant impact or prevalence. Those service providers are also already required to assess the risk to children from other non-priority content they have identified on their service through the risk assessment, which includes any other content which presents a material risk of significant harm to an appreciable number of children, and protect them from this. We are retaining this requirement for companies subject to the child safety duties, given the Government's intention to ensure the Bill provides a higher level of protection for children.

DCMS Committee Recommendation – Content that is harmful to adults (Para 21)

33. ***The Bill should include non-exhaustive, illustrative lists of preventative and remedial measures beyond takedowns for both illegal and 'legal but harmful' content, proportionate to the risk and severity of harm, to reflect a structured approach to content (referenced in paragraph 9). This could include tagging or labelling, covering, redacting, factchecking, deprioritising, nudging, promoting counter speech, restricting or disabling specific engagement and/or promotional functionalities (such as likes and intra- and cross-platform sharing) and so on.***

Government Response

34. We welcome the Committee's recommendation that illustrative lists of measures beyond takedown should be added to the Bill. In response we have added non-exhaustive, indicative areas which indicate the types of measures that companies subject to the safety duties can take to fulfil their safety duties for illegal content and protecting children:

a) Regulatory compliance and risk management arrangements

b) Design of features, functionalities and algorithms

c) Policies on terms of use

d) Policies on user access to the service or to particular content present on the service, including blocking users from accessing the service or particular content

e) Content moderation, including taking down content

f) Functionalities allowing users to control the content they encounter

g) User support measures

h) Staff policies and practices.

35. Ofcom's codes of practice will cover these areas, recommending that companies take steps in the different areas to fulfil their duties for illegal content and protecting children, where it is proportionate to do so.

36. For content that is harmful to adults, Category 1 service providers will be able to decide their own policies on how to handle each type of harmful content. They will have to say how their terms of service respond to the risks that they have identified in their risk assessments. They will have to make clear which types of content they intend to remove and limit access to. They will also have to say which types of content will be recommended or promoted. They will be obliged to enforce those terms of service consistently. It is not therefore appropriate to list possible areas of remedial action in the legislation.

DCMS Committee Recommendation – Content that is harmful to adults (Para 22)

37. ***We recommend that the definition of content that is harmful to adults should explicitly include content that undermines, or risks undermining, the rights or reputation of others, national security, public order and public health or morals, as also established in international human rights law.***

Government Response

38. We thank the Committee for their consideration of this issue. The Bill will cover many of the issues raised in this recommendation through the illegal and legal but harmful safety duties. A number of the priority offences set out in the Bill are crimes that undermine peoples' rights, national security and public order including threats to kill, hate crime, terrorism and public order offences. The priority harms will cover many issues that pose a threat to public health, including some types of harmful misinformation such as anti-vaccination content. These measures will have an overall positive impact on many of the societal issues raised by the Committee.

39. These harms have been designed to give platforms and Ofcom sufficient legal certainty about the types of content they are required to address. Broadening the definition to include wider harms to society and could incentivise excessive takedown of legal material. It is essential that the legislative measures uphold and protect the fundamental right to freedom of expression.

40. Instead, as set out above, we have removed the requirement for Category 1 service providers to address non-priority harmful content (other than to report its presence on their services to Ofcom). Instead, every category of content that is harmful to adults covered by companies' safety duties will be set out in legislation. This change will make it clearer to such companies which types of content they are required to address and give Parliament full oversight of what is defined as content that is harmful to adults, in addition to protecting peoples' right to freedom of expression by reducing the risks of over-removal of legal content.

41. To be included, these priority categories of legal but harmful content will need to present a material risk of significant harm to adults in the UK. We consider this an appropriate definition of this type of content in line with the Bill's purpose to reduce harm caused by content on companies' services. Priority categories will cover some types of harmful misinformation and disinformation such as anti-vaccination content and other health misinformation that poses a threat to public health. Category 1 services will also be under a duty to report emerging harms, i.e. content which is harmful to adults which is not priority content to Ofcom.

42. This approach provides sufficient flexibility to update the regulatory framework as new harms develop, and gives legal certainty to Category 1 service providers. The Secretary of State would also be able to designate content of the type mentioned by the Committee where such content presents a material risk of significant harm to adults.

DCMS Committee Recommendation – Content that is harmful to adults (Para 23)

43. ***Our definitions also provide meaningful ways to proportionately mitigate the impacts of harms to democracy. We recommend that, in addition to the factors listed above, the definition for content that is harmful to adults should be further clarified to explicitly account for any intention of electoral interference and voter suppression when considering a speaker's intentionality and the content's accuracy, and account for the content's democratic importance and journalistic nature when considering the content's context.***

Government Response

44. We welcome the Committee's consideration of this important issue. It is, and always will be, an absolute priority to protect our democratic and electoral processes. The Government has robust systems in place that bring together Government, civil society and private sector organisations to monitor and respond to electoral interference in whatever form it takes to ensure that our democracy stays open, vibrant and transparent.

45. Although there is a role for regulation, this needs to be carefully balanced with the need to protect freedom of expression and the legitimate public debate also crucial to a thriving democracy. As highlighted above, we are concerned about the difficulties in defining content that causes harm to democracy in a way that would give legal certainty to platforms and Ofcom. Content such as satire could be caught by such a definition, and this could incentivise excessive takedown of legal material.

46. However, the Government takes a range of actions to ensure the integrity of elections which helps to take care of the concerns behind your recommendation. The cross-Government Defending Democracy programme brings together capabilities and expertise across departments and the security and intelligence agencies to protect and secure UK democratic processes from interference. Ahead of major democratic events, the Defending Democracy programme stands up the Election Cell. This is a strategic coordination and risk reporting structure that works with relevant organisations to identify and respond to emerging issues.

47. The Counter Disinformation Unit based in DCMS is an integral part of the Election Cell structure and undertakes work to understand the extent, scope and the reach of misinformation and disinformation during elections. The Unit works closely with social media companies to quickly identify and respond to potentially harmful content on their platforms, including removing content in line with their terms and conditions and promoting authoritative sources of information.

48. We know that certain states seek to exploit and undermine our open system through online disinformation and have made clear that it is absolutely unacceptable for anyone to interfere in our democracy. We are working to ensure the UK has a refreshed and sufficiently robust legal framework to provide enhanced powers to address and respond to the threat from foreign interference. Work on new legislative proposals to specifically tackle foreign interference is ongoing and will be introduced as soon as parliamentary time allows. All liberal democracies face this challenge, not just the UK, and we work

together with those nations to tackle it. We will continue to call out and respond to malign activity, including any attempts to interfere in our democratic processes, alongside our international partners.

49. These initiatives are complemented by provisions in the Elections Bill, including the clarification and updating of the undue influence offence which can include deceiving an elector about the administration of an election or referendum with the intention of that elector voting in a particular way or refraining from voting. The Bill also extends the "imprint" requirement to online campaign material, thus increasing transparency in digital campaigning for voters. A digital imprint will need to include the promoter's details or the details of the person or organisation on behalf of whom the material is published, helping voters to identify who is behind digital political material.

DCMS Committee Recommendation – Designation of types of harm (Para 25)

50. ***The Government should add a new Schedule to the Bill providing at least the most relevant types of illegal content and non-exhaustive illustrative lists of proportionate preventative and remedial measures to mitigate and manage risk. It should also provide, in another new Schedule, a detailed procedure for designating new and/or additional offences that constitute illegal content in the Bill through regulations. Alongside the Bill, the Government should issue example Regulations to illustrate how this process would work and ensure it is done consistently post-implementation.***

Government Response

51. We thank the Committee for their recommendation. On 7 February 2022, we announced that priority offences would be included on the face of the Bill. This means that, in addition to CSEA and terrorism offences, companies subject to the safety duties must also put in place proactive measures to tackle the list of further priority offences in Schedule 7. Those companies will need to design and operate their services to prevent users encountering priority illegal content. Beyond the priority offences, those services will need to ensure that they have effective systems and processes in place to quickly take down other illegal content targeting individuals once it has been reported or they become aware of its presence.

52. The Secretary of State will have the power to amend the list of priority offences by secondary legislation, which will be subject to the affirmative resolution procedure to allow for maximum parliamentary scrutiny. The Secretary of State will be able to add further offences by regulations when she considers it appropriate because of the prevalence, risk or severity of the harm associated with that content. Evidence from Ofcom and relevant stakeholders will form part of this consideration.

53. As noted above, the Bill will include non-exhaustive areas within which companies might be expected to take measures, where proportionate, to meet their illegal content duties. These areas are listed above and will include content moderation and policies on user access.

DCMS Committee Recommendation – Designation of types of harm (Para 28)

54. ***We recommend that the Government produce new Schedules detailing procedures for designating, by regulations, content that is harmful to children and content that is harmful to adults. Any regulations designating types of harm should define the harms and provide non-exhaustive illustrative lists of factors and proportionate preventative and remedial measures.***

Government Response

55. We welcome the Committee's recommendations. The Bill already sets out that the Secretary of State will be able to designate categories of priority content that is harmful in secondary legislation where he or she considers that there is a material risk of significant harm to adults or children in the UK arising from content of that description. This approach of using secondary legislation, as opposed to setting out in the schedules in primary legislation, allows the list of harms to be flexible and updatable in the face of changing and emerging harms.

56. The Bill also sets out the parliamentary procedure through which the Secretary of State can designate categories in secondary legislation. Regulations made under this power will be subject to the affirmative resolution procedure to allow for maximum parliamentary scrutiny, except in urgent cases (when the made affirmative procedure will allow new categories to be designated quickly, subject to approval by both Houses within 28 days).

57. The Bill also sets out that Ofcom should publish reports on the suitability of the categories of priority harmful content at least once every three years. The Secretary of State will also consult with Ofcom before making regulations.

58. With regard to the second part of the Committee's recommendation about setting out preventative and remedial measures, please note our responses above addressing this issue. In addition, the Bill has been updated to include specific references to age assurance technologies, including age verification, as examples of the measures companies may need to use to protect children and meet their safety duties.

59. The reasons why it would not be appropriate to specify possible areas of remedial action for content that is harmful to adults are set out in paragraph 36 above.

DCMS Committee Recommendation – Designation of types of harm (Para 29)

60. ***The Joint Committee on the Draft Online Safety Bill has made several recommendations regarding the Secretary of State's powers. We agree with their recommendations to clarify the power to make exemptions for services in scope and remove the power to modify Codes of Practice and give guidance to Ofcom. However, the Secretary of State's powers when making regulations to designate types of harm should be amended further for legal but harmful content to protect freedom of expression. All regulations making designations under "content that is harmful to children" and***

"content that is harmful to adults" should be subject to the affirmative procedure. This will provide an important, additional safeguard for freedom of expression, recognising the need for additional parliamentary oversight in this area.

Government Response

61. We welcome the Committee's consideration of this issue. We are keen to ensure that Parliament has an ongoing role in scrutinising the Online Safety Bill and associated regulations. In the draft Bill, the first regulations made to specify descriptions of primary priority content that is harmful to children, priority content that is harmful to children and priority content that is harmful to adults were to be made under the affirmative resolution procedure, with subsequent regulations made under the negative resolution procedure.

62. Following the recommendation of this Committee, we are updating the Bill so that all subsequent regulations to designate types of harm are subject to the affirmative resolution procedure. This is with the exception of cases where the Secretary of State considers that there is an urgent need to specify a new description of harmful content. In those circumstances, as noted above, the regulations will be subject to the made affirmative procedure.

63. For the codes of practice, it is important that the Government remains able to direct Ofcom to modify a code of practice for reasons relating to Government policy. It is important that there are suitable, transparent checks and balances to ensure that the implementation of the regime by the independent regulator, Ofcom, delivers the policy intent that will be decided by the democratically-elected government.

64. We intend that this power would only be used in exceptional circumstances, and the Bill contains limits to the power to ensure that there is the right balance between Government oversight and regulatory independence. The Secretary of State would only be able to use this power to direct Ofcom to modify a code at the end of the process, rather than at any stage, and the details of any direction given would be published alongside the modified code. Any code would be subject to parliamentary scrutiny before it came into force.

65. Separately, the power to give guidance to the regulator is not intended to, nor does it allow for, the Secretary of State to interfere with Ofcom's operational independence. It is intended to be used to publicly set out the Government's high-level strategic expectations of Ofcom, where deemed necessary, in order to provide more certainty on the Government's intentions to both Ofcom and businesses. Ofcom must have regard to guidance issued by the Secretary of State, but is not bound by it.

DCMS Committee Recommendation – Designation of types of harm (Para 30)

66. ***We recommend that the Government should take forward the commitments made by the Prime Minister and work with charities, campaign organisations and children's advocacy groups to identify, define and address legal but harmful content, such as content that advocates self-harm and types of online violence against women and girls, that are not currently illegal.***

Government Response

67. We welcome the Committee's interest in this important issue. We continue to work closely with charities, campaign organisations and children's advocacy groups to identify, define and address legal but harmful content.

68. Following the publication of the Online Harms White Paper, the Government held a 12-week consultation from April to June 2019 and received over 2,400 responses. The Department held 100 consultation meetings with a wide range of key stakeholders, including groups championing children's online safety and representing children and young people themselves.

69. The Government has commissioned research to build the evidence base on priority harms to children online. This includes a rapid evidence assessment which will review the evidence base about the prevalence and impact of a wide range of harmful content to children. The Government has also commissioned a piece of qualitative research which will explore the impacts of harmful content on children through conducting focus groups with parents and professionals working with children, and in-depth interviews with children themselves.

70. The Government will consult Ofcom on priority categories of content that is harmful to children and they will be expected to draw on evidence and views from relevant parties. Ofcom will also have a duty to carry out reviews on the incidence and severity of harm caused to children and adults on regulated services. Ofcom will have flexibility in how it develops the codes of practice and will consult with a range of stakeholders as part of the development of these codes.

71. The Bill has robust mechanisms to ensure companies' take action in relation to content that advocates violence against women, both where that content meets the threshold of a criminal offence and where it does not but still causes significant harm. There are also requirements for protecting children from this type of content. A number of priority offences that have been explicitly linked to violence against women and girls such as offences relating to sexual images (i.e revenge and extreme pornography), and harassment and stalking offences, are listed as priority illegal offences on the face of the Bill.

72. Following the Government's interim response to the Law Commission's review, 'Modernising the Communications Offence', the Bill has been updated to include the recommended harm-based communications, false communications and threatening communications offences by the Law Commission. In addition the Law Commission's recommended cyberflashing offence will also be taken forward through the Bill. The Government continues to assess the recommendations on self-harm and epilepsy abuse. We have also indicated that content that promotes self-harm and suicide but which does not reach the criminal threshold will be listed as priority categories of legal but harmful content for adults and children.

73. Separately, our cross-Government Tackling Violence Against Women and Girls Strategy commits the Government to: investing in high quality, evidence-informed prevention projects, including in schools; a national communications campaign with a focus on educating young people about healthy relationships and ensuring victims can access support; an additional £1.5m this year for specialist support services and increasing our funding for helplines, such as the Revenge Porn Helpline.

Enforcing the regime

Summary

- This chapter focuses on Ofcom's powers to gather information and enforce the regime and the right of users to bring claims in court.
- The Government has been clear that delivering greater transparency, trust and accountability is at the heart of the new regulatory framework and that Ofcom must have strong enforcement powers to hold companies to account.
- The Committee's recommendations in this area focus on strengthening and providing more clarity about Ofcom's information-gathering and enforcement powers.
- Since publication of the draft Bill, we have developed the Bill further to:
  - bring forward senior management liability for non-compliance with information requests so that the offence comes into force shortly after Royal Assent.
  - refine the Use of Technology power (now known as the 'Notices to deal with terrorism content or CSEA content (or both)').
  - require user-user service providers to set out that users have a right of action in court when their content is removed in breach of a user-user service provider's terms of service.
- We have also decided not to support the establishment of a permanent Joint Committee on Digital Regulation.

DCMS Committee Recommendation – Transparency and information-gathering powers (Para 33)

74. ***We recommend that the Government provide Ofcom with the power to conduct confidential auditing or vetting of a service's systems to assess the operation and outputs in practice (itself or through an independent third party) in Chapter 3 of the Bill. Alongside the power to request generic information about how "content is disseminated by means of a service", the Government should also include in Section 49(b) a non-exhaustive list of specific information that may be requested, subject to non-disclosure, including:***

a) ***The provider's objectives and the parameters for a system's outputs, (such as maximising impressions, views, engagement and so on);***

b) ***Their metrics for measuring performance and references of success;***

c) ***The datasets on which systems are developed, trained and refined, including for profiling, content recommendation, moderation, advertising, decision making or machine learning purposes;***

d) ***How these datasets are acquired, labelled, categorised and used, including who undertakes these tasks;***

e) ***Data on and the power to query a system's outputs, including to request or scrape information on said outputs given particular inputs.***

Government Response

75. We welcome the Committee's detailed recommendations in this important area. We have clarified in the Bill that Ofcom will have the power to audit a service's systems and processes in order to assess compliance and/or develop an understanding of risk.

76. Beyond this, we consider that the Bill will enable Ofcom to require the types of information suggested by the Committee. Ofcom will be able to request this information, through their information gathering powers under clause 85. These powers are very broad and as such we are satisfied that Ofcom will be equipped to gather the information it needs to effectively regulate the sector. There are strict limitations on Ofcom's disclosure of such material. Ofcom will be prohibited from disclosing information obtained from companies without consent, unless very clearly defined exemptions apply.

DCMS Committee Recommendation – Transparency and information-gathering powers (Para 34)

77. ***We also recommend that the online safety regime should require providers to have designated compliance officers, similar to financial services regulation and which we have advocated previously, in order to bake compliance and safety by design principles into corporate governance and decision-making.***

Government Response

78. We welcome the Committee's interest in ensuring the regime is enforced properly. We want senior executives in the tech sector to take these new responsibilities seriously and be held to account if they do not properly engage with the regime. Although not every company will need a designated compliance officer, we are confident the framework will operate to ensure that senior executives properly engage with their companies' new responsibilities.

79. Senior managers face criminal proceedings if they do not ensure their company properly engages with Ofcom and complies with its information requests. This will push senior executives to make sure Ofcom has the information it needs to regulate the tech sector effectively and enforce where needed. These criminal sanctions will now be in force shortly after Royal Assent so that senior managers can be quickly held to account by Ofcom.

80. We are also introducing additional information-related criminal offences, including for companies who provide false or misleading information or employees who lie when being interviewed by Ofcom. The package of enforcement powers and information offences will ensure Ofcom has access to the information it needs to do its job and promote strong compliance with the wider regime.

DCMS Committee Recommendation – Enforcement powers (Para 38)

81. ***We recommend that the Government provide greater clarity about the use of enforcement powers contained in the Bill. First, it should make explicit that these powers apply only to in-scope services.***

Government Response

82. We thank the Committee for their recommendation. Ofcom can take enforcement action against providers of regulated services if they breach any of their duties under the Bill. Ofcom can also take enforcement action against any entity or person (not just regulated providers) who fails to comply with Ofcom's information requests or skilled persons' reviews. It can only utilise business disruption measures (including blocking) in relation to regulated services. The extent and scope of Ofcom's enforcement powers are already clearly stated in the Bill.

83. Further, Ofcom will consult and publish enforcement guidelines covering this new regime, which will provide more detail on how it intends on using its enforcement powers. Stakeholders will be able to respond to the consultation as they see fit. We therefore do not intend to make any changes to the Bill on this point.

DCMS Committee Recommendation – Enforcement powers (Para 39)

84. ***Second, it should redraft the use of technology notices by more tightly defining the scope and application of the power, the actions required to bring providers to compliance and a non-exhaustive list of criteria that might constitute a test as to whether the use of such power is proportionate, such as:***

a) ***The evidential basis for intervention (including the time period this evidence covers);***

b) ***The level of risk and severity of harm that exists on the service and the existing systems used to identify and mitigate or manage these risks;***

c) ***The implications for human rights, including freedom of expression and user privacy;***

d) ***The cost to the service relative to factors such as its user base and revenue.***

Government Response

85. We are making improvements to Ofcom's 'Use of Technology notice' power in line with the Committee's feedback. These notices are now known as 'Notices to deal with terrorism content or CSEA content (or both)'. We have amended the Bill to ensure that this power provides a robust response to the extremely concerning prevalence of CSEA online, while also ensuring there are built-in safeguards to ensure users' rights are upheld.

86. We have amended the Bill to refine this power. Instead of the existing test, Ofcom will be able to issue a notice requiring technology to be implemented if it considers it *necessary and proportionate*. This will ensure it has the power to use this power when it considers it is needed to tackle CSEA or terrorism content.

87. We agree that stringent safeguards must regulate Ofcom's application of this power. Ofcom must also have had regard to a list of factors, including the level of risk of harm to users, the functionalities of the service and whether any less intrusive measures are likely to achieve the same reduction in illegal content. We believe this will ensure this power is used effectively and proportionately and will also allow Ofcom to draw on a wider range of evidence.

DCMS Committee Recommendation – Enforcement powers (Para 40)

88. ***Third, with regards to business disruption measures, we recommend that the Government provide greater clarity to other services in the supply chain by bringing forward more detailed proposals for how this would work in practice. This should include:***

a) ***Time frames and consultation requirements;***

b) ***Due consideration for human rights implications, including the unintended coverage of legal content;***

c) ***Consideration for the costs to services that might be required to enact the measure; and***

d) ***Processes for updating consumers.***

Government Response

89. We note the Committee's detailed recommendations. The Bill provides Ofcom with the necessary powers to oversee and enforce the new regime. It also places an obligation on Ofcom to publish enforcement guidelines to give further clarity and transparency on how it will exercise its powers. This will include more detail on how Ofcom will exercise its right to apply to the courts for business disruption measures. We expect Ofcom will engage extensively with relevant stakeholders when developing the guidance, and Ofcom will publish a consultation before finalising its enforcement guidelines.

90. It is worth noting that the courts will specify the exact requirements of each business disruption order, including timeframes for implementation. The courts also have to consider the rights of all the parties involved (including UK users) and be satisfied that the order is proportionate to the risk of harm.

DCMS Committee Recommendation – Enforcement powers (Para 41)

91. ***The Government should also give consideration to, and evaluate in its response to this Report, whether these powers are appropriately future-proofed given the advent of technology like VPNs and DNS over HTTPs.***

Government Response

92. We welcome and agree with the Committee's recommendation. The provisions have been drafted in tech-neutral language. We are confident that we have future-proofed these provisions to cover future technological changes.

DCMS Committee Recommendation – Enforcement powers (Para 42)

93. ***We recommend that the Government include a provision in the Bill to mandate publication of a breach notice by a service. This should include details of their breaches against the duty of care and be available to view on the platform.***

Government Response

94. We thank the Committee for their recommendation. Ofcom is required to publish details of its enforcement activity, unless it is not appropriate for publication (e.g. for public interest reasons). We believe this will bring sufficient transparency to Ofcom's enforcement activity. As such, we do not propose to require regulated providers to publish details of any breaches they have committed on their service.

DCMS Committee Recommendation – Redress and judicial review (Para 44)

95. ***The Government must provide further clarity on the subject of redress and judicial review to ensure the effective implementation of the Online Safety Bill. We recommend that the Government should include a provision in the Bill to clarify that the right of eligible entities to make super-complaints before Ofcom is without prejudice to the right of individuals to access courts and make judicial complaints on a case-by-case basis for breaches of user-to-user and search service providers' duties of care laid down in the Bill and other acts or omissions that are unlawful under other applicable laws. The Government should amend Clauses 15(3) and 24(3) to impose a duty on providers to operate a complaints procedure that gives users notice of any restriction on their ability to access and use the service, along with the reasons for the restriction.***

Government Response

96. We welcome the Committee's recommendations regarding user redress. We can assure the Committee that the super-complaint mechanism is not intended to override users' ability to take action against a company in court. It is important that users are able to access effective redress mechanisms and the super-complaints mechanism is only one part of a package of user redress mechanisms set out in the Bill.

97. In response to the Committee, however, we are requiring user-user service providers to set out in terms of service that users have a right of action in court where their content is removed in breach of a service provider's terms of service.

98. With regard to the recommendation that providers should be required to notify users if their content is removed from a service, Ofcom will be required to set out how service providers subject to the safety duties can comply with their user redress duties, where applicable, in codes of practice. We expect that, where proportionate, this could include provision for those service providers to give users notice of any restriction on their ability to access and use the service, along with the reasons for the restriction.

99. This will not necessarily be proportionate in all cases, for example for very small service providers. As such we do not intend to specify this level of detail in legislation, however we do expect that Ofcom will consider whether to include steps such as these when developing the codes of practice.

DCMS Committee Recommendation – Parliamentary scrutiny and oversight (Para 45)

100. ***Parliamentary scrutiny of the ongoing work on the UK's regime for digital regulation by the Department for Digital, Culture, Media and Sport, regulators and associated bodies is vital. However, we consider that this is best serviced by the existing, independent, cross-party select committees and evidenced by the work we have done and will continue to do in this area. We recommend that the Government should scrap any plans to introduce a Joint Committee to oversee online safety and digital regulation.***

Government Response

100. We agree that effective parliamentary oversight has an important role to play in this fast moving space. We welcome the contributions that have been made by the DCMS Select Committee, its Committee on Online Harms and Disinformation, the Lords Communications and Digital Committee, and the Joint Committee on the Draft Online Safety Bill.

101. On the online safety legislation, ongoing scrutiny will provide reassurance that the online safety regulatory regime is having the impact we envisage. This is a groundbreaking regulatory framework. It will affect millions of people across the UK and services from across the globe will be required to act, including some of the world's biggest companies with unprecedented reach and power. Parliamentary scrutiny will ensure that Ofcom's approach as the regulator, the Government's role, and the response of in-scope services are all held to account in an appropriate manner.

102. Utilising the depth of expertise in both Houses will be an effective way to deliver post legislative scrutiny. The Government is not intending to legislate for a new committee via the Online Safety Bill. However, the Government intends to work with Parliament to support scrutiny of the Online Safety Act in a way that utilises the skills and expertise in both Houses. This will ensure that Parliament is able to scrutinise thoroughly matters related to keeping people safe online with the breadth of scope and pace required.

103. In addition, we see real risks of duplication in creating a Joint Committee focused on digital regulation more broadly. Such a committee would cut across the work of existing parliamentary committees that are already well placed to scrutinise digital regulation and for this reason we do not support the recommendations on this from the Joint Committee on the Draft Online Safety Bill and Lords Communications and Digital Committee.