HM Government

Government Response to the Report of the Joint Committee on the Draft Online Safety Bill

March 2022

CP 640

Government Response to the Report of the Joint Committee on the Draft Online Safety Bill

Presented to Parliament by the
Secretary of State for Digital, Culture, Media and Sport
by Command of Her Majesty

March 2022

CP 640

This publication is available at www.gov.uk/official-documents

Any enquiries regarding this publication should be sent to us at onlineharms.coordination@dcms.gov.uk

ISBN 978-1-5286-3231-7
E02721600 03/22

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of Her Majesty's Stationery Office

Contents

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 2019.[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. We are pleased to agree with the Joint Committee on the core objectives of the Bill. 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 services 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 which doesn't 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 future-proofed and subject to ongoing scrutiny.

Pre-legislative scrutiny process

4. This Bill takes a novel and world-leading approach to prevent harm on the internet. The government has engaged consistently with a wide cross-section of interested parties as we have developed the legislation. The pre-legislative scrutiny process has been a critical and valuable part of that engagement, including the detailed scrutiny provided of the drafting itself.

5. We are very grateful for the Joint Committee's thorough and robust work, and to the stakeholders and parliamentarians who have shared their thoughts on the legislation. They have drawn together a remarkable level of expertise from across Parliament, reflecting the significant impact parliamentarians have already had on the development of this policy since the publication of the White Paper in 2019. Equally, their evidence sessions showed a comprehensive, constructive and insightful approach to the issues and debates. We are confident that the outcome of this scrutiny is a bill that is sustainable, workable, proportionate, and which will create a significant step-change in the experience people have online. The Joint Committee has had an important role in helping us to reach this outcome.

Summary of the Joint Committee's recommendations and government responses

6. The Joint Committee's report made a number of recommendations about the draft Bill. The following paragraphs summarise these recommendations under key themes and set out at a high level the government's response to each. We are grateful for the thinking behind the Joint Committee report and are making significant changes to the Bill as a result. We have strengthened our legislation by incorporating 66 of the Joint Committee's recommendations. Further details are provided in the following chapters.

Key points in our response: Protecting users from illegal content & activity

7. As stated above, one of the Bill's key aims is to tackle criminal activity online. During the pre-legislative scrutiny process, we have heard the concerns raised by those affected by fraudulent advertising online, and agree with the Joint Committee's concerns about this activity. In recognition of the detrimental and devastating effects that fraudulent advertisements can have on those affected by them, we will introduce a new standalone duty in the Bill requiring Category 1 (the largest and highest risk services in scope) services to take action to minimise the likelihood of fraudulent adverts being published on their service. This will make it far harder for fraudsters to advertise their scams online, and if Category 1 services fail to take adequate action they could face stringent enforcement action.

8. We also support the Joint Committee's recommendation of including priority offences on the face of the primary legislation. The government welcomes the committee's recommendations on the issue of online fraud and we can confirm that fraud offences will be included in this list. 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 services, which in turn will force

rapid action against illegal harms. However, it is important to note that these services will still have to remove illegal content relating to criminal offences that do not appear on the list of priority offences, where it is flagged to them by users.

Anonymity

9. The Joint Committee, as well as many of the stakeholders that we have engaged with during the development of this legislation, has recommended further measures to tackle anonymous abuse online. We recognise this concern, and so have strengthened the Bill's provisions by including two new additional duties on Category 1 services (the largest companies in scope) to ensure adult users are given the option to verify their identity, and tools to have more control over the legal content that they see as well as who they interact with. This would include providing adults with the option not to interact with unverified users. This will protect the right to anonymity for those who benefit from it – such as victims of domestic abuse or whistleblowers – whilst ensuring users have control over their online experience. Empowering users in this way provides a safer internet, whilst protecting freedom of expression by reducing the need for controls on harmful content accessed by consenting adults.

Communications offences

10. The government is also grateful for the hard work carried out by the Law Commission. As we announced on 4th February 2022, we accept the recommended offences on harm-based communications, false communications and threatening communications, as laid out in the Law Commission's report. These new offences will be taken forward in the Online Safety Bill, and will help ensure that the criminal law is focused on the most harmful behaviour whilst protecting freedom of expression, by ensuring that communications that are intended to contribute to the public interest are not prosecuted. In addition, as the Prime Minister has indicated, we welcome the Law Commission's recommended offence of cyberflashing. The government has also confirmed that we will include it in the Online Safety Bill.

Child Safety

11. Protecting children's safety and rights is at the heart of the Online Safety Bill. We therefore accept the points made by the Joint Committee on the need to ensure children are protected from access to pornography on dedicated sites as well as on social media. To address this, we have added a provision to the Bill to require all service providers that publish or display pornographic content on their services to prevent children from accessing this content. All services included in this provision will be subject to the same enforcement measures as other services in the Bill.

Enforcement

12. To achieve our aim of making the UK the safest place in the world to go online, we must give Ofcom robust powers to enforce the online safety framework. We fully support the Joint Committee's belief that the senior executives of services need to be held accountable for the actions these services take. With this in mind, the legislation will no longer defer the power to bring in the criminal sanctions for failures to comply with information notices, and this will instead be introduced as soon as possible after Royal Assent (likely to be two months after). This will ensure that online safety becomes, and remains, a key topic of discussion in boardroom conversations amongst senior executives, giving it the priority it deserves.

13. When taking enforcement action, Ofcom can require a company with a substandard risk assessment to take measures to mitigate risks it has missed at the same time as it redoes its risk assessment. This change will further encourage services in scope of the safety duties to put safety at the heart of their service, whilst promoting innovation and development.

Next steps

14. The work of the Joint Committee has been vital in ensuring that this Bill will achieve what it set out to establish: an internet that tackles criminal activity; protects children and young people from harmful and inappropriate content; and allows adults to make informed choices about exposure to potentially harmful content whilst protecting freedom of expression. The Bill will be proportionate and risk-based, to account for the diversity of services in the online space, and will support the UK's thriving and innovative digital sector.

Structure, objectives and over-arching considerations

SUMMARY

- This chapter deals with the legislative structure of the Bill, and with its overall objectives.
- The Joint Committee's recommendations in this area focused on restructuring the Bill, so that its aims and objectives are set out upfront, to provide context for the more detailed duties which follow later in the legislation. The Joint Committee also recommended that, contrary to the position in the draft Bill, Ofcom's codes of practice should be mandatory.
- Firstly, in terms of the objectives of the Bill, the government believes that the Bill already meets the Joint Committee's objectives. Although we acknowledge the Committee's view that the legislation is complex, we believe that this is necessary in order to produce a framework which can effectively deal with the range and diversity of online businesses that the Online Safety Bill will apply to.
- Secondly, in response, we have made a number of changes to simplify the structure and provisions:
  - Setting out in the legislation categories of measures that companies should take action in order to meet their safety duties. These categories will be covered in more detail in Ofcom's codes of practice;
  - Restructuring the risk assessments and safety duties so that the duties on platforms are clearer; and
  - Simplifying the definition of harmful content that is harmful to adults, by removing the duties associated with non-priority content.
- Finally, to the Committee's point about binding codes of practice, we will not be changing their status, as our approach drives innovation within safety technology, and has precedent in other regimes.

Joint Committee Recommendation – The draft Bill (Para 52 & 60-61):

15. *We recommend the Bill is restructured. It should set out its core objectives clearly at the beginning. This will ensure clarity to users and regulators about what the Bill is trying to achieve and inform the detailed duties set out later in the legislation. These objectives should be that Ofcom should aim to improve online safety for UK citizens by ensuring that service providers:*

a. *comply with UK law and do not endanger public health or national security;*

b. *provide a higher level of protection for children than for adults;*

c. *identify and mitigate the risk of reasonably foreseeable harm arising from the operation and design of their platforms;*

d. *recognise and respond to the disproportionate level of harms experienced by people on the basis of protected characteristics;*

e. *apply the overarching principle that systems should be safe by design whilst complying with the Bill;*

f. *safeguard freedom of expression and privacy; and*

g. *operate with transparency and accountability in respect of online safety.*

16. *We recommend that the Bill be restructured to contain a clear statement of its core safety objectives—as recommended in paragraph 52. Everything flows from these: the requirement for Ofcom to meet those objectives, its power to produce mandatory codes of practice and minimum quality standards for risk assessments in order to do so, and the requirements on service providers to address and mitigate reasonably foreseeable risks, follow those codes of practice and meet those minimum standards. Together, these measures amount to a robust framework of enforceable measures that can leave no doubt that the intentions of the Bill will be secured.*

17. *We believe there is a need to clarify that providers are required to comply with all mandatory codes of practice as well as the requirement to include reasonably foreseeable risks in their risk assessments. Combined with the requirements for system design we discuss in the next chapter [of the Joint Committee's report], these measures will ensure that regulated services continue to comply with the overall objectives of the Bill—and that the Regulator is afforded maximum flexibility to respond to a rapidly changing online world.*

Government Response

18. The draft Bill was the culmination of a long process of policy development, consultation and engagement with a diverse range of stakeholders to develop a comprehensive regulatory framework to improve online safety. Such comprehensive regulation of this relatively young and extremely dynamic sector has not been attempted before. The challenge has been to legislate to achieve detailed policy objectives in a way that provides sufficient legal certainty to all services about their obligations in a way which is risk-based and proportionate, future-proofed and enforceable by the regulator.

19. The Bill has been significantly developed from the draft published in May 2021. The framework has been adapted in the light of views expressed on the draft Bill and the Bill has been expanded through the addition of a number of standalone provisions to target specific online issues, as detailed throughout this response.

20. We are grateful to the Joint Committee for scrutinising the draft Bill's objectives and structure, as well as its drafting. We agree with all of the objectives the Joint Committee has set out, and believe that the Bill already encapsulates and should achieve these objectives.

21. In terms of the specific restructure that the Committee suggested, we believe that using these objectives *as the basis for Ofcom's regulation* would delegate unprecedented power to a regulator. We do not believe that reformulating this regulatory framework in this way would be desirable or effective. In particular, the proposal would leave Ofcom with a series of high-level duties, which would likely create an uncertain and unclear operating environment. Such an environment could also lead to a reduction in legal certainty for services, Ofcom and users and to a greater likelihood of legal challenges, as well as potential delays to the vital safety benefits for users that this legislation will bring.

22. We appreciate that the Committee believes the Bill to be overly complicated. Legislating for a largely unprecedented, comprehensive, future-proofed and enforceable framework, has required the creation of a range of targeted duties and a series of new definitions. We have simplified some aspects of the framework, such as the definition of content that is harmful to adults, in light of the Committee's comments. However, the fact that the Bill is complicated does not mean the framework itself will in practice be overly complicated for services, ranging from social media giants to the smallest online forums, to comply with and for Ofcom to enforce. Ofcom's codes of practice (and any associated guidance) will provide detail and clarity for services as to what steps they need to take to comply with their legislative duties, taking into account their risk profile.

Joint Committee Recommendation – Enforcement against the safety duties (Para 325):

23. *The Bill should be amended to clarify that Ofcom is able to take enforcement action if it identifies a breach of the safety duties, without requiring a provider to redo a risk assessment.*

Government Response

24. Our aim is to ensure that Ofcom has robust and effective enforcement measures across the regime. Ofcom will be able to require a company with a substandard risk assessment to take measures to mitigate risks it has missed at the same time as it redoes its risk assessment. This will ensure that a service subject to the safety duties is accountable to Ofcom in taking appropriate remedial action – within deadlines set by Ofcom. If such a service fails to take such steps, Ofcom can pursue further enforcement action, including imposing a fine and/or pursuing business disruption measures (including blocking).

Joint Committee Recommendation – Codes of practice (Para 358):

25. *The Bill should be amended to make clear that codes of practice should be binding on providers. Any flexibility should be entirely in the hands of and at the discretion of the Regulator, which should have the power to set minimum standards expected of providers. They should be subject to affirmative procedure in all cases.*

Government Response

26. While we note the Committee's position on Ofcom's codes of practice, we consider it is preferable to leave greater flexibility in the framework. Firstly, there is no obvious precedent of codes being binding. Therefore, any binding rules would have to be in legislation rather than codes.

27. More importantly, in such a dynamic and innovative sector, it is important that all services should be able to implement measures as set out in the codes *or* take alternative steps to those in the codes if they operate effectively to protect users. This will help ensure innovation in the sector is not hindered, and users are protected in a constantly evolving online world.

28. We should be clear that no matter which route a company chooses to take – following the codes or achieving equivalent outcomes – it will be for Ofcom to determine a company's compliance and thus ensure they are meeting minimum standards for ensuring user safety.

29. However, we have made changes to the Bill to provide more detail on measures that could be taken to comply with the safety duties – such as regulatory compliance, the design of functionalities and policies on terms of use. We have also strengthened the provisions that require services to fully document and justify any alternative measures taken. We consider this will make it easier for Ofcom to evaluate the steps taken by a given service and aid enforcement action.

Joint Committee Recommendation – Codes of practice (Para 359):

30. *Ofcom should start working on codes of practice immediately, so they are ready for enforcement as soon as the Bill becomes law. A provisional list of codes of practice, including, but not necessarily limited to, those listed in Box 2 above should be included on the face of the Bill. Some of the codes should be delegated to co-designated bodies with relevant expertise, which would allow work on multiple codes to happen simultaneously and thus the entire endeavour to be completed more quickly. Once the codes of practice are completed, they should be published.*

Government Response

31. We want Ofcom to be flexible in how it develops the codes of practice, including being able to combine or separate the codes in ways that are most helpful for all services in scope of the safety duties. Providing a list of codes on the face of the Bill would remove that flexibility. Stakeholders have previously raised concerns about having multiple codes of practice, which could be burdensome and hard to follow. We will continue to work closely with Ofcom to ensure that the regulatory regime is implemented as quickly as possible.

Joint Committee Recommendation – Accessibility and consistency of terms and conditions (Para 184 & 185):

32. *We recommend that the Bill mandates service providers to produce and publish an Online Safety Policy, which is referenced in their terms and conditions, made accessible for existing users and made prominent in the registration process for new users. This Online Safety Policy should: explain how content is promoted and recommended to users, remind users of the types of activity and content that can be illegal online and provide advice on what to do if targeted by content that may be criminal and/or in breach of the service providers' terms and conditions and other related guidelines.*

33. *The Online Safety Policy should be produced in an accessible way and should be sent to all users at the point of sign up and, as good practice suggests, at relevant future points. "Accessible" should include accessible to children (in line with the Children's code), where service providers allow child users, and accessible to people with additional needs, including physical and learning disabilities. Ofcom should produce a code of practice for service providers about producing accessible and compliant online safety policies and on how they should make them available to users to read at appropriate intervals in line with best practice (for example, when the user is about to undertake an activity for the first time or change a safety-relevant setting).*

Government Response

34. The government agrees that it is important for users to have information about services' safety policies. The Online Safety Bill requires all services in scope of the safety duties to explain in their terms and conditions how users will be protected from illegal content. Similarly, all services likely to be accessed by children will be required to set out how children are to be prevented from, or protected from, encountering content that is harmful to children. Category 1 services will have to explain how their terms and conditions for legal content that harms adults reflect their risk assessments and which kinds of harmful content will be prohibited, limited or promoted to users. The Bill requires all of these terms and conditions to be clear and accessible.

35. Ofcom will need to set out how services subject to the safety duties can comply with these duties in codes. For example, companies could present terms and conditions to users when they sign up for a service and in other appropriate circumstances.

Who does the Bill apply to?

SUMMARY

- This chapter focuses on which services are in scope of the regulatory framework.
- The government has always been clear that the focus of the legislation is user-to-user services and search services, where there is a real risk of harm to users in the UK. The types of services and content in scope must remain targeted on riskier services, where there is a gap in regulation or liability, and where the government can make the greatest intervention.
- The Joint Committee's recommendations in this area focused on two types of recommendations – expanding the content in scope of the regime, and then the requirements on in-scope services, in particular on encrypted services.
- We are grateful for the Committee's extensive scrutiny of online fraud and fraudulent advertising. Since publication of the draft Bill, we have considered this issue further, and will now bring fraudulent advertising into the scope of the Bill by introducing a new standalone duty to require the highest risk and highest reach platforms (including large search services) to minimise the likelihood of fraudulent adverts being published on their service, and protect their users.

Joint Committee Recommendation – Categorisation (para 246):

36. *We recommend that the categorisation of services in the draft Bill be overhauled. It should adopt a more nuanced approach, based not just on size and high-level functionality, but factors such as risk, reach, user base, safety performance, and business model. The draft Bill already has a mechanism to do this: the risk profiles that Ofcom is required to draw up. We make recommendations in Chapter 8 about how the role of the risk profiles could be enhanced. We recommend that the risk profiles replace the "categories" in the Bill as the main way to determine the statutory requirements that will fall on different online services. This will ensure that small, but high risk, services are appropriately regulated; whilst guaranteeing that low risk services, large or small, are not subject to unnecessary regulatory requirements.*

Government Response

37. Risk is built into the categorisation process set out in the Bill. In making regulations for Category 1 thresholds, the Secretary of State must take into account the likely impact of the number of users of a service and its functionalities on the level of risk of harm to adults from content that is harmful to adults disseminated by means of the service. Reach is an important factor in assessing risk as online abuse can cause more harm when it reaches a larger audience. In responding to evolving and changing risks, the Secretary of State also has flexibility to ensure the various categories can be adapted to reflect these emerging threats.

38. Nevertheless, the government agrees that requirements on companies must reflect the varied ways in which a service can have an increased possibility of causing harm. Regulatory requirements in the Bill will be proportionate to the findings of companies' risk assessments, which will be guided by the risk profiles set out in Ofcom's sectoral risk assessment. Many of the factors set out by the Joint Committee will be sub-components of risk, but not specified at a legislative level.

39. We want the Bill to be targeted and proportionate for businesses and Ofcom and do not wish to impose disproportionate burdens on small companies**.**

Joint Committee Recommendation – End-to-End encryption (Para 257):

40. *The government needs to provide more clarity on how providers with encrypted services should comply with the safety duties ahead of the Bill being introduced into Parliament.*

Government Response

41. The UK government supports the responsible use of encryption: it is critical to the protection of UK citizens' privacy online and billions of people use it every day for a range of services, including banking and commerce.

42. However, we are also committed to ensuring the UK is the safest place in the world to be online, and that all services, including end-to-end encrypted ones, have a responsibility to protect public safety. End-to-end encryption should not be rolled out without appropriate safety mitigations, for example, the ability to continue to detect known CSEA imagery. Platforms must increase their engagement with the issue of protecting child safety in end-to-end encrypted environments. Without greater investment in safety solutions, there will be detrimental consequences for tech companies' ability to reduce the proliferation of child sexual abuse material on their platforms, to protect children from being groomed online, and to safeguard victims.

43. Within the regulatory framework, companies will be responsible for ensuring *all* of their services, including encrypted ones, comply with safety duties in legislation, informed by Ofcom's codes of practice*.* We appreciate the committee's desire for greater clarity in this area. However, there will not be a one-size fits all approach as the risk presented will depend on a range of factors, including the wider design of a service. It would therefore not be appropriate to detach encrypted services and deal with them differently.

44. Work is underway within government, through the Safety Tech Challenge Fund and connected initiatives, to support the development of technologies that can detect CSEA within end-to-end encrypted environments, whilst respecting user privacy. We are also exploring whether the pace at which industry develops these technologies can be increased.

Joint Committee Recommendation – End-to-End encryption (Para 258):

45. *We recommend that end-to-end encryption should be identified as a specific risk factor in risk profiles and risk assessments. Providers should be required to identify and address risks arising from the encrypted nature of their services under the Safety by Design requirements.*

Government Response

46. The government agrees that it is important to factor end-to-end encryption into risk assessments. Companies must already consider the risks arising from the design and operation of their services, functionalities and how their services are used. They will need to risk assess changes to systems in order to put in place proportionate mitigations. Assessing the risks arising from end-to-end encryption will be an integral part of this process. Ofcom will produce guidance to assist companies in carrying out their risk assessments.

Joint Committee Recommendation – Exclusion of paid-for advertising from scope (Para 268-271):

47. *The exclusion of paid-for advertising from the scope of the Online Safety Bill would obstruct the government's stated aim of tackling online fraud and activity that creates a risk of harm more generally. Excluding paid-for advertising will leave service providers with little incentive to remove harmful adverts, and risks encouraging further proliferation of such content.*

48. *We therefore recommend that Clause 39(2) is amended to remove "(d) paid-for advertisements" to bring such adverts into scope. Clause 39(7) and Clause 134(5) would therefore also have to be removed.*

49. *Ofcom should be responsible for acting against service providers who consistently allow paid-for advertisements that create a risk of harm to be placed on their platform. However, we agree that regulating advertisers themselves (except insofar as they come under other provisions of the Bill), individual cases of advertising that are illegal, and pursuing the criminals behind illegal adverts should remain matters for the existing regulatory bodies and the police.*

50. *We recommend that the Bill make clear Ofcom's role will be to enforce the safety duties on providers covered by the online safety regulation, not regulate the day-to-day content of adverts or the actions of advertisers. That is the role of the Advertising Standards Authority. The Bill should set out this division of regulatory responsibility.*

Government Response

51. The government recognises the huge problem caused by scam adverts and online fraud and the devastating impact it can have on individuals, and welcomes the Joint Committee's recommendations in this area.

52. We have amended the Bill to introduce a new duty requiring Category 1 services, as well as large search services, to put in place proportionate systems and processes to prevent users encountering fraudulent adverts on their service. This applies to any adverts appearing on their service, whether these are controlled by the company itself or an advertising intermediary. Ofcom will produce a code of practice outlining the steps services should take, providing more detail on how companies can comply with this new duty.

53. This change will make it harder for fraudsters to advertise scams online, and protect people from this devastating crime. Further details will be set out in Ofcom's codes, however we expect Category 1 services and large search services to put in place a range of measures. These measures could include processes to verify that advertisers are who they say they are, with checks to ensure only firms regulated by the FCA (or those who have had their financial promotions approved by an FCA regulated firm) are able to communicate financial promotions. They could also include swift processes for removing fraudulent adverts.

54. We have also removed the exemption for 'paid-for advertising' from the definition of user-generated content. This will ensure that user-generated content on social media that is paid to be promoted, for example a boosted post, is subject to the Bill's safety duties.

55. We do not intend to introduce requirements on companies to tackle other forms of harmful advertising in the Bill. The Online Advertising Programme will examine the full spectrum of both illegal and legal harms caused by a lack of transparency and accountability across the online advertising supply chain. The Programme will consider the role of all actors across the ecosystem, including intermediaries, services and publishers not currently covered by regulation, to provide a holistic review of the regulatory framework. We are therefore introducing a duty that ensures that the government's approach to regulating online advertising is aligned with wider comprehensive reform aimed at improving trust and reducing harm across the system.

56. This is only one part of the solution. The government is continuing to explore additional legislative and non-legislative solutions to tackle fraud in the round. This work is led across government by the Home Office, in collaboration with industry, regulators and consumer groups. The Home Office is developing an ambitious Fraud Strategy.

Joint Committee Recommendation – Economic harms (Para 275):

57. *We recognise that economic harms other than fraud, such as those impacting consumers, and infringement of intellectual property rights, are an online problem that must be tackled. However, the Online Safety Bill is not the best piece of legislation to achieve this. Economic harms should be addressed in the upcoming Digital Competition Bill. We urge the government to ensure this legislation is brought forward as soon as possible.*

Government Response

58. We agree that the Online Safety Bill is not the place to address these issues. The government set out its proposals for a new pro-competition regime in a public consultation which closed in Autumn of last year. We are currently analysing the responses to that consultation. We will legislate when parliamentary time allows.

Joint Committee Recommendation – Secretary of State powers (Para 376):

59. *The power for the Secretary of State to exempt services from regulation should be clarified to ensure that it does not apply to individual services.*

Government Response

60. The Bill already makes clear that the Secretary of State can exempt services that meet a certain description. In most cases this would cover more than one service, unless there was a service with a totally unique risk profile.

61. It would not be desirable to limit this power to cases where there is more than one service that meets a description, as it could mean that a unique, low-risk service cannot be exempt. This would add undue and disproportionate burdens to services that do not pose a risk of harm. As such, we do not consider that any changes are necessary.

What harms are in scope?

SUMMARY

- This chapter focuses on the types of harmful content and activity that the regulatory framework is due to tackle.
- The government has been clear that content and/or activity is in scope of the legislation if it poses a material risk of harm to individuals in the UK.
- The Joint Committee's recommendations in this area focused on online anonymity and societal harm.
- Whilst anonymity in and of itself is not necessarily harmful, both the government and the Joint Committee has heard compelling evidence about the impact of online abuse, and online anonymous abuse. As a result, the government will strengthen the safety duties, by adding two new additional duties on the largest companies in scope to provide adults with optional user verification and user empowerment tools.

Joint Committee Recommendation – Content and activity (Para 68):

62. *We recommend that references to harmful "content" in the Bill should be amended to "regulated content and activity". This would better reflect the range of online risks people face and cover new forms of interaction that may emerge as technology advances. It also better reflects the fact that online safety is not just about moderating content. It is also about the design of platforms and the ways people interact with content and features on services and with one another online.*

Government Response

63. The government agrees with the necessity of capturing a broad range of online interaction. The Bill already covers harmful content and activity through its existing drafting. All online activity is facilitated by content and, therefore, by imposing duties on services to address illegal and harmful content, the Bill will cover both activity and content. Taking the examples mentioned by the Committee, the Bill directly requires service providers to assess the risks of harm linked to how their services are designed and to consider how a comprehensive range of functionalities and how their services are used affect risk. They

will have to look at how their services allow users to forward or share content, send direct messages or play games with other users or to express views on other users' content through "likes" or voting or rating for example.

64. For the avoidance of doubt, changes have been made to the Bill making it indisputable that the duties of care cover not only content but also activity. For example, the overview of Part 3 clause specifies that services providers' duties of care apply in relation to both content and activity on their services, and other clauses specify that the safety duties apply to the way the service is operated and used as well as the content on it.

Joint Committee Recommendation – Anonymity and traceability (Para 92 – 94):

65. *We recommend that platforms that allow anonymous and pseudonymous accounts should be required to include the resulting risks as a specific category in the risk assessment on safety by design. In particular, we would expect them to cover, where appropriate: the risk of regulated activity taking place on their platform without law enforcement being able to tie it to a perpetrator, the risk of 'disposable' accounts being created for the purpose of undertaking illegal or harmful activity, and the risk of increased online abuse due to the disinhibition effect.*

66. *We recommend that Ofcom be required to include proportionate steps to mitigate these risks as part of the mandatory code of practice required to support the safety by design requirement we recommended in paragraph 82. It would be for them to decide what steps would be suitable for each of the risk profiles for online services. Options they could consider might include (but would not be limited to):*

a. *Design measures to identify rapidly patterns of large quantities of identical content being posted from anonymous accounts or large numbers of posts being directed at a single account from anonymous accounts;*

b. *A clear governance process to ensure such patterns are quickly escalated to a human moderator and for swiftly resolving properly authorised requests from UK law enforcement for identifying information relating to suspected illegal activity conducted through the platform, within timescales agreed with the regulator;*

c. *A requirement for the largest and highest risk platforms to offer the choice of verified or unverified status and user options on how they interact with accounts in either category;*

d. *Measures to prevent individuals who have been previously banned or suspended for breaches of terms and conditions from creating new accounts; and*

e. *Measures to limit the speed with which new accounts can be created and achieve full functionality on the platform.*

67. *We recommend that the code of practice also sets out clear minimum standards to ensure identification processes used for verification protect people's privacy—including from repressive regimes or those that outlaw homosexuality. These should be developed in conjunction with the Information Commissioner's Office and following consultation with groups including representatives of the LGBTQ+ community, victims of domestic abuse, journalists, and freedom of expression organisations. Enforcement of people's data privacy and data rights would remain with the Information Commissioner's Office, with clarity on information sharing and responsibilities.*

Government Response

68. The government is grateful to the Committee for the work on the issue of anonymity and in particular for the powerful testimony of a number of stakeholders on the issue of online abuse. We recognise the concern that many people have about anonymity online. We are pleased to announce a number of changes to the Bill that will go further to tackle online abuse and anonymous online abuse, whilst protecting anonymity for those who may need it for legitimate purposes, or wish to use it for harmless purposes.

69. Taking the Committee's three points in turn:

a. Firstly, the Committee recommended that platforms which allow anonymous and pseudonymous accounts should have to consider these factors specifically within the risk assessment. This is already covered by the Bill as companies already need to risk assess harms that are associated with functionalities that allow users to create anonymous profiles.

b. Secondly, the Committee recommended that Ofcom be obliged to include proportionate steps to mitigate these risks as part of a mandatory code of practice. We agree that much of this detail should be included in the codes of practice, but do not believe it necessary to include this obligation on the face of the Bill.

c. Thirdly, on the interaction with data protection, as the Committee says enforcement of people's data privacy would remain with the Information Commissioner's Office. However, we intend for Ofcom to engage with the ICO and all relevant stakeholders on these issues when developing their codes. Ofcom will be required to consult with the ICO when developing the codes of practice.

70. To further address the concerns about online abuse, and in particular anonymous online abuse, the government has further strengthened the Bill. There are two new additional duties on the Category 1 services: to provide adults with optional user verification and user empowerment tools. The first additional duty requires Category 1 services to provide their users with an option to verify their identity. The second requires Category 1 services to provide tools to give users more control over the legal but harmful content they see and the ability to choose who they interact with. This means that users who have verified their ID will be able to ensure that they are only able to interact and see content from other verified users.

71. The new duties will help provide robust protections for adults, and take account of potential impacts on vulnerable adults. The new provisions will also help manage concerns regarding freedom of expression, as both provisions allow users to choose which content they see instead of requiring companies to place restrictions on the legal but harmful content.

72. We note the issue highlighted by the Committee in relation to the risk of regulated activity taking place on a service without law enforcement being able to tie it to a perpetrator. There are existing legal frameworks to support police in the identification of online offenders. We are considering whether there is anything further that can be done within the online safety framework to support this.

Joint Committee Recommendation – Societal harm and the role of safety by design (Para 111):

73. *Disinformation and misinformation surrounding elections are a risk to democracy. Disinformation which aims to disrupt elections must be addressed by legislation. If the government decides that the Online Safety Bill is not the appropriate place to do so, then it should use the Elections Bill which is currently making its way through Parliament.*

Government Response

74. The government agrees that misinformation and disinformation surrounding elections are a risk to democracy and it is vital to address this 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 governmental, civil society, and private sector organisations to monitor and respond to interference in whatever form it takes to ensure that our democracy stays open, vibrant and transparent. 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.

75. The government takes a range of actions to ensure the integrity of elections. 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, systems and institutions from interference. This involves work across four strategic objectives to:

- Protect and secure UK democratic processes, systems, and institutions from interference, including from cyber, personnel, and physical threats;
- Strengthen the integrity of elections, including by working through regulators;
- Encourage respect for open, fair and safe democratic participation by tackling intimidation; and
- Promote fact-based and open public discourse, both online and in the traditional media, including tackling disinformation.

76. 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. The Counter Disinformation Unit based in DCMS is an integral part of this structure and undertakes work to understand the extent, scope and the reach of misinformation and disinformation. 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.

77. 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. The government remains committed to ensuring a sufficiently robust legal framework is in place to address and respond to the threat from foreign interference. Work to develop enhanced powers to tackle such interference is ongoing and legislation will be introduced as soon as parliamentary time allows.

78. All liberal democracies face this challenge, not just the UK, and we work together 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. This includes taking forward the UK government's commitment from the 2021 Summit for Democracy to share best practice with like minded partners on the best approaches to countering disinformation.

79. As the Committee notes, 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. 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. The government

is also building audience resilience to misinformation and disinformation through media literacy initiatives and undertaking a wide-ranging programme of research to understand the scale, scope, and impact of online manipulation.

Joint Committee Recommendation – Societal harm and the role of safety by design (Para 112):

80. *The Information Commissioner, Elizabeth Denham, has stated that the use of inferred data relating to users' special characteristics as defined in data protection legislation, including data relating to sexual orientation, and religious and political beliefs, would not be compliant with the law. This would include, for example, where a social media company has decided to allow users to be targeted with content based on their data special characteristics without their knowledge or consent. Data profiling plays an important part in building audiences for disinformation, but also has legitimate and valuable uses. Ofcom should consult with the Information Commissioner's Office to determine the best course of action to be taken to investigate this and make recommendations on its legality.*

Government Response

81. As the former Information Commissioner noted, the UK's data protection regime already contains protections for individuals. Ofcom and the ICO will be collaborating closely on the privacy and personal data aspects of the regulatory framework. This will ensure the ICO's oversight of data protection and Ofcom's oversight of the Online Safety regulatory framework work effectively together.

Illegal harms to adults

SUMMARY

- The government has always been clear that one of the main aims of the legislation is to require services to prevent the proliferation of illegal content and activity online.
- The Joint Committee's recommendations in this area focused on changing the structure of the Bill with regards to illegal harms, and the reform of the criminal law.
- Since publication of the draft Bill, we have developed the Bill further to address the Committee's concerns:
  - Firstly, we include all priority illegal offences in the primary legislation, with an affirmative power for the Secretary of State to update this. This will ensure clarity for platforms and users, and speed up the implementation of the regime. This includes offences covering revenge pornography, harassment and fraud.
  - Secondly, the government has now accepted the Law Commission's recommended harm-based, false communications and threatening communications offences. In addition the government has also confirmed that it has accepted the cyberflashing offence, and will include all of these offences in the Online Safety Bill.

Joint Committee Recommendation – Scope of illegal content (Para 126-127):

82. *We believe the scope of the Bill on illegal content is too dependent on the discretion of the Secretary of State. This downplays the fact that some content that creates a risk of harm online potentially amounts to criminal activity. The government has said it is one of the key objectives of the Bill to remove this from the online world.*

83. *We recommend that criminal offences which can be committed online appear on the face of the Bill as illegal content. This should include (but not be limited to) hate crime offences (including the offences of "stirring up" hatred), the offence of assisting or encouraging suicide, the new communications offences recommended by the Law Commission, offences relating to illegal, extreme pornography and, if agreed by Parliament, election material that*

is disinformation about election administration, has been funded by a foreign organisation targeting voters in the UK or fails to comply with the requirement to include information about the promoter of that material in the Elections Bill.

Government Response

84. The government accepts the Committee's recommendation to include the list of priority offences in primary legislation. We have updated the Bill accordingly. The Secretary of State will be able to update the list of priority offences through secondary legislation, using the affirmative procedure associated with the Child Sexual Exploitation and Abuse (CSEA) and Terrorism provisions. This will ensure the list can be updated to respond to emerging illegal harms or to add new offences.

85. This change will ensure that it is clear from the outset the priority offences that service providers will have obligations for. It addresses the calls for greater clarity heard during pre-legislative scrutiny and will increase the pace of implementation of the Bill. The government will be able to bring the illegal content duties into force more quickly, and therefore services subject to the safety duties will be obliged to assess their services for the risks of illegal content, put in place systems and processes to mitigate them, and protect their users at an earlier date than would have been possible under the draft Bill.

86. The list of priority offences to be included has been developed using criteria set out in the draft Bill. These criteria are:

a. The prevalence of such content on regulated services;

b. The risk of harm being caused to UK users by such content; and

c. The severity of that harm.

87. The list also takes into account the extent to which services can feasibly implement systems to proactively tackle listed offences.

88. In accordance with the Committee's recommendations, we have included offences on hate crime, assisting or encouraging suicide and extreme pornography in the list of priority offences. For a full list of categories of offences that will be included, please see Annex A. Specific offences within these categories will be set out on the face of the Bill.

89. The new communication offences and disinformation about election administration offences recommended by the Law Commission are not being included as priority offences. This is because these offences rely heavily on a user's intent making it challenging for services to proactively identify this content, without significant additional context.

90. Crucially, this change does not impact the duty to address other offences that were also included in the draft Bill. For any criminal offences that have individuals as victims which do not appear on the list of priority offences, services will still have to remove such content where it is flagged to them or they otherwise become aware of it.

Joint Committee Recommendation – Power to designate priority illegal content (Para 148):

91. *We recommend that the Secretary of State's power to designate content relating to an offence as priority illegal content should be constrained. Given that illegal content will in most cases already be defined by statute, this power should be restricted to exceptional circumstances, and only after consultation with the Joint Committee of Parliament that we recommend in Chapter 9, and implemented through the affirmative procedure. The Regulator should also be able to publish recommendations on the creation of new offences. We would*

expect the government, in bringing forward future criminal offences, to consult with Ofcom and the Joint Committee as to whether they should be designated as priority illegal offences in the legislation that creates them.

Government Response

92. The government supports the aim of this recommendation. As noted above, we have included the "priority offences" within the Bill, meaning that this list will be subject to full Parliamentary scrutiny. The Secretary of State will retain the ability to designate additional offences as priority offences via the affirmative procedure. The Secretary of State will be able to add further priority offences by regulations only 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 also form part of this consideration.

Joint Committee Recommendation – Reform of the criminal law (Para 136):

93. *We endorse the Law Commission's recommendations for new criminal offences in its reports, Modernising Communications Offences and Hate Crime Laws. The reports recommend the creation of new offences in relation to cyberflashing, the encouragement of serious self-harm, sending flashing images to people with photo-sensitive epilepsy with intent to induce a seizure, sending knowingly false communications which intentionally cause non-trivial emotional, psychological, or physical harm, communications which contain threats of serious harm and stirring up hatred on the grounds of sex or gender, and disability. We welcome the Secretary of State's intention to accept the Law Commission's recommendations on the Communications Offences. The creation of these new offences is absolutely essential to the effective system of online safety regulation which we propose in this report. We recommend that the government bring in the Law Commission's proposed Communications and Hate Crime offences with the Online Safety Bill, if no faster legislative vehicle can be found. Specific concerns about the drafting of the offences can be addressed by Parliament during their passage.*

Government Response

94. We welcome the Committee's recommendation related to the Law Commission review, that the government bring in the Law Commission's proposed communication offences through the Online Safety Bill. We appreciate the extensive work that the Law Commission has led over the past four years to ensure that criminal law better protects victims from harmful and abusive communications online.

95. As recently announced in our interim response to the Law Commission's report, 'Modernising the Communications Offences,' the government has accepted the recommended harm-based, false communications, and threatening communications offences. These new offences will ensure that criminal law is able to capture a multitude of harmful communications online and offline, while protecting free expression. They also help deliver the government's objective of making the UK the safest place to be online. The offences will be brought into law through the Online Safety Bill. In addition, the government has also confirmed that it has accepted the Law Commission's recommended cyberflashing offence, which will be taken through the Online Safety Bill. Adding this offence is an important step forward in ensuring better protection for users of online services, including women and girls, who are disproportionately impacted by this behaviour.

96. The Law Commission recommended a further three offences – hoax calls, epilepsy trolling and self-harm. The Department for Digital, Culture, Media and Sport and the Ministry of Justice are continuing to carefully consider the remaining offences and accompanying

recommendations. We recognise the Joint Committee's concern in these areas, particularly following evidence from witnesses who highlighted the seriousness of these types of communications and the severe impact they can have. We will continue to assess these offences and appropriate legislative vehicles, ahead of issuing a full response to the Law Commission's report.

97. The Committee has also recommended that the government take forward the hate crime offences within the Online Safety Bill. The Law Commission has led a separate review regarding the hate crime offences, which has been sponsored by the Home Office. The Law Commission published its final report in December and the government will publish its interim response to the report in due course.

Joint Committee Recommendation – Reform of the criminal law (Para 138):

98. *The government must commit to providing the police and courts with adequate resources to tackle existing illegal content and any new offences which are introduced as a result of the Law Commission's recommendations.*

Government Response

99. One of the aims of the Online Safety Bill is to tackle and reduce the amount of illegal content online, which is expected in the longer term to reduce the demand on law enforcement and the courts. Ultimately, decisions about the allocation of police resources and deployment of officers are for Chief Constables and Police and Crime Commissioners. However, it is worth noting that the Home Office continues to fund specialist investigation teams such as the Police Online Hate Crime Hub, the Social Media Hub and the Counter Terrorism Internet Referral Unit.

100. To ensure that the impacts of the Online Safety Bill are considered and planned for, to make best use of public funds and to make sure the service provision within the justice system is not jeopardised, a Justice Impact Test (JIT) has been completed. This was cleared by the Ministry of Justice in May 2021. The JIT has recently been updated to incorporate an assessment of the Law Commission recommendations as well some other policy developments and is under review by the Ministry of Justice.

Joint Committee Recommendation – Identifying illegal content (Para 144):

101. *We recommend that Ofcom be required to issue a binding code of practice to assist providers in identifying, reporting on and acting on illegal content, in addition to those on terrorism and child sexual exploitation and abuse content. As a public body, Ofcom's code of practice will need to comply with human rights legislation (currently being reviewed by the government) and this will provide an additional safeguard for freedom of expression in how providers fulfil this requirement. With this additional safeguard, and others we discuss elsewhere in this report, we consider that the test for illegal content in the Bill is compatible with an individual's right to free speech, given providers are required to apply the test in a proportionate manner that is set out in clear and accessible terms to users of the service.*

Government Response

102. We welcome the Committee's conclusion that the test for illegal content in the Bill is compatible with an individual's right to free speech. The government can confirm that Ofcom's codes of practice will assist services in identifying and acting on illegal content.

103. As set out in the chapter on the powers of the regulator, we are not aware of any precedent of codes being binding. Therefore, any binding rules would have to be in legislation rather than codes. Given the criminal law and considerations on content moderation are constantly evolving, it would neither be appropriate, nor future-proof, to set these considerations in legislation. Nevertheless, we are confident that Ofcom's guidance in the codes of practice will be effective.

Joint Committee Recommendation – Identifying illegal content (Para 145):

104. *We recommend that the highest risk service providers are required to archive and securely store all evidence of removed content from online publication for a set period of time, unless to do so would in itself be unlawful. In the latter case, they should store records of having removed the content, its nature and any referrals made to law enforcement or the appropriate body.*

Government Response

105. The government sympathises with the concerns raised by the Joint Committee, but data retention for law enforcement purposes is already strictly regulated, and the Online Safety Bill is not the place to revisit it. 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 there is no requirement to retain any data under the Act. Services 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 under the IPA.

106. We note the issue highlighted by the Committee in relation to the risk of regulated activity taking place on a platform without law enforcement being able to attribute it to a perpetrator. There are existing legal frameworks to support police in the identification of online offenders, but we will consider if there is anything further within the online safety framework to support this.

Joint Committee Recommendation – Online fraud (Para 194 & 195):

107. *We welcome the inclusion of fraud and scams within the draft Bill. Prevention must be prioritised and this requires platform operators to be proactive in stopping fraudulent material from appearing in the first instance, not simply removing it when reported. We recommend that Clause 41(4) is amended to add "a fraud offence" under terrorism and child sexual exploitation and abuse offences and that related Clauses are similarly introduced or amended so that companies are required to proactively address it. The government should consult with the regulatory authorities on the appropriate offences to designate under this section. The government should ensure that this does not compromise existing consumer protection regulation.*

108. *The Bill must make clear that ultimate responsibility for taking action against criminal content remains with the relevant regulators and enforcement bodies, with Ofcom reporting systemic issues relating to platform design and operation—including in response to "super complaints" from other regulators. The Bill should contain provisions requiring information-sharing and regulatory cooperation to facilitate this.*

Government Response

109. The government can confirm that the list of priority offences that will be included in the primary legislation will include fraud offences.

110. In terms of the Committee's second point, about regulatory overlap, we are grateful for the cooperation we have received from other regulators such as the Information Commissioner's Office and the Competitions & Markets Authority. We agree that Ofcom will need to work closely with other regulators, as well as law enforcement, to avoid any regulatory overlap.

Legal but harmful (adults)

SUMMARY

- This chapter deals with the way in which harmful content which does not meet the criminal threshold is dealt with, when accessed by adults.
- The Joint Committee's recommendations in this area focused on providing greater clarity and direction to Category 1 services about the steps they must take to tackle this content.
- First, the Joint Committee proposed narrowing the types of legal content that Category 1 services must address. Under the recommendations, Category 1 services would only address legal content if it fell into one of a number of set categories closely related to offences (although the content would not need to meet the criminal threshold).
- Second, the Joint Committee recommended empowering Ofcom to set binding codes of practice that services must follow to mitigate the risk of harm from this content, including through content moderation.
- Government is concerned that the Committee's recommendations could undermine protections for freedom of expression. However, in response, we have developed the Bill further to ensure greater clarity about services' regarding legal but harmful content. Specifically, the Bill will now:
  - Remove the requirement for Category 1 services to address harmful content accessed by adults, beyond the priority harms which will be set out in secondary legislation. This provides clarity about the harms that services must address and will reduce the risk of Category 1 services taking an overly broad approach to what is considered harmful;
  - Provide greater clarity about what Category 1 services' terms and conditions for harmful content must cover, to ensure they can be held fully accountable to these;
  - Require Category 1 services to set out how their terms and conditions respond to their risk assessments; and

– Add a new duty for Category 1 services to provide user empowerment measures, which are designed to give adults greater choice over the content that they see as well as the people that they interact with. This may allow users to choose not to see certain types of harmful content, even if the site they are on accepts it.

Joint Committee Recommendation – Replacing Clause 11 (Para 176-177, 180):

111. *We recommend that Clause 11 of the draft Bill is removed. We recommend that it is replaced by a statutory requirement on providers to have in place proportionate systems and processes to identify and mitigate reasonably foreseeable risks of harm arising from regulated activities defined under the Bill. These definitions should reference specific areas of law that are recognised in the offline world, or are specifically recognised as legitimate grounds for interference in freedom of expression. For example, we envisage it would include:*

a. *Abuse, harassment or stirring up of violence or hatred based on the protected characteristics in the Equality Act 2010 or the characteristics for which hatred may be an aggravating factor under Crime and Disorder Act 1998 and section 66 of the Sentencing Act 2020;*

b. *Content or activity likely to cause harm amounting to significant psychological distress to a likely audience (defined in line with the Law Commission offence);*

c. *Threatening communications that would lead a reasonable person to fear that the threat might be carried out;*

d. *Knowingly false communications likely to cause significant physical or psychological harm to a reasonable person;*

e. *Unsolicited sending of pictures of genitalia;*

f. *Disinformation that is likely to endanger public health (which may include antivaccination disinformation);*

g. *Content and activity that promotes eating disorders and self-harm;*

h. *Disinformation that is likely to undermine the integrity and probity of electoral systems*

112. *As with the other safety duties, we recommend that Ofcom be required to issue a mandatory code of practice to service providers on how they should comply with this duty. In doing so they must identify features and processes that facilitate sharing and spread of material in these named areas and set out clear expectations of mitigation and management strategies that will form part of their risk assessment, moderation processes and transparency requirements. While the code may be informed by particular events and content, it should be focused on the systems and processes of the regulated service that facilitates or promotes such activity rather than any individual piece of content.*

113. *We recommend that additions to the list of content that is harmful should be by statutory instrument from the Secretary of State. The statutory instrument should be subject to approval by both Houses, following a report from the Joint Committee we propose in Chapter 9. Ofcom, when making recommendations, will be required by its existing legal obligations to consider proportionality and freedom of speech rights. The Joint Committee should be specifically asked to report on whether the proposed addition is a justified interference with freedom of speech rights.*

Government Response

114. Clause 11 has been designed to hold Category 1 services accountable to their terms and conditions, while empowering users to make informed decisions about the services they use. Category 1 services will be required to set clear terms and conditions about how they will protect their users and Ofcom will ensure these are properly enforced. This approach will increase transparency about services' content moderation processes, preventing such services from arbitrarily removing content that is not prohibited on their service.

115. The government has a number of concerns about the approach proposed by the Joint Committee, particularly relating to protections for freedom of expression and delegating power to an independent regulator to determine rules limiting the spread of legal content online.

116. The Joint Committee's proposals would constitute a significant interference with freedom of expression, obliging services to remove or minimise the presence, prominence, and spread of legal content. They would introduce different standards for legal material online and offline so a newspaper would be free to publish content that would be prohibited on an online service. There could be a significant chilling effect as it may incentivise Category 1 services to remove or limit material that was not in fact harmful because of concerns about complying with their duties.

117. The duty proposed by the Committee would delegate an inappropriate degree of power to Ofcom to determine what legal content is permissible online, and how companies should treat this. Requiring services to address legal content that is harmful to adults would undermine the risk-based and proportionate principles on which the Bill is based. It is right that the duty for legal content that is harmful to adults should only extend to the highest risk, highest reach services. Legal but harmful material is more likely to spread quickly and reach large numbers of people on these services.

118. However, we are making a number of changes to the Bill's provisions for legal but harmful content which align with the Committee's recommendations to ensure these provisions go far enough in addressing harm and to provide greater clarity about the actions Category 1 services must take with regard to legal content. This will ensure that Category 1 services can be held fully accountable for the terms and conditions, while ensuring they are clear about their approach to managing risk.

119. We will specify in legislation a requirement for Category 1 services to set out in their terms and conditions how they treat legal but harmful content by reference to the kind of treatment, ranging from prohibiting it, through limiting it in some way to actively promoting it. Category 1 services will also need to explain how their terms and conditions respond to the findings of their risk assessments for legal but harmful content. These changes will result in more clarity for users about the extent to which they will be protected from harm on a Category 1 service.

120. The approach to defining content that is harmful to adults will also be refined. All the types of harmful content that Category 1 services are required to address will be set out in regulations subject to approval by both houses. Category 1 services will continue to be required to report emerging harms to the regulator and where appropriate these harms will be quickly added to the regulations. This will help to address some of the Committee's concerns about the need for a fixed list, and the complexity of the Bill, by giving Category 1 services and users greater legal certainty over which harms will be addressed.

121. In addition, Category 1 services will also be required to implement user empowerment tools. These tools would also allow users more control over which types of legal but harmful content they see, and which other users they interact with, empowering users to protect themselves from harmful content. This mirrors the choices people have in the offline world.

Harms to children

SUMMARY

- The government has always been clear that the protection of children is at the heart of the regime, and children will be offered a higher level of protection.
- The Joint Committee's recommendations in this area focused on the definition of harmful content for children, commercial pornography and age assurance technologies.
- Since publication of the draft Bill, we have developed the Bill further, to strengthen the protections for children within the Bill:
  - To close the loophole for commercial pornography services, we have added an additional standalone provision to require these services to prevent children from accessing pornographic content;
  - To simplify the definition of non-designated content that is harmful to children, and make the obligations on services clearer; and
  - To ensure that age assurance technologies are referred to as a way of complying with the safety duties.

Joint Committee Recommendation – Definition of content harmful to children (Para 202):

122. *Recognising the key objective of offering a higher level of protection for children than adults, we support the inclusion of a broad definition of content that is harmful to children. At the same time, we believe the definition should be tightened. We recommend that Clauses 10(3) to (8) are revised. Content and activity should be within this section if it is specified on the face of the Bill, in regulations or there is a reasonably foreseeable risk that it would be likely to cause significant physical or psychological distress to children who are likely to encounter it on the platform.*

Government Response

123. As we have made clear, the protections for children are at the heart of the regulatory framework. With regards to the drafting suggestions made by the Committee, for regulated user-to-user and search services, content is already harmful to children if it is designated as primary priority content or priority content through regulations, or if it satisfies the definition of content that is harmful to children in the Bill. However, we have considered the Committee's proposals, and the revised Bill introduces a simplified definition of harmful content at clause 52 which is content "of a kind which presents a material risk of significant harm to an appreciable number of children in the United Kingdom". Harm is still defined as physical or psychological harm as set out in clause 186. The definition will still include harm which occurs as the result of how content is disseminated, indirect harm to children, and harm which is a result of content that is related to an individual's characteristics or membership of a group, which are also set out in clause 186. These are not mentioned in the Committee's proposed definition, but we consider are important to have clearly outlined in the legislation.

Joint Committee Recommendation – Definition of content harmful to children (Para 203):

124. *As with other duties, we recommend that key, known risks of harm to children are set out on the face of the Bill. We would expect these to include (but not be limited to) access to or promotion of age-inappropriate material such as pornography, gambling and violence material that is instructive in or promotes self-harm, eating disorders or suicide, and features such as functionality that allows adults to make unsupervised contact with children who do not know them, endless scroll, visible popularity metrics, live location, and being added to groups without user permission.*

Government Response

125. The government still believes that setting out the priority harms to children in secondary legislation is the better approach. Firstly, we believe that it is right to conduct research and ensure adequate consultation with child safety groups who have expertise in this area, once the framework has been set. The Bill requires Ofcom, as the regulator, to publish frequent reports and the Secretary of State must consult Ofcom on the proposed categories of harm to children. This will ensure that the priority harms, as well as their definitions, are evidence-based and reflect the experiences of and greatest risks to children online.

126. Secondly, the government believes that as well as the use of an ongoing and underpinning evidence-basis, the harms to children require a future-proofed and flexible legislative mechanism. As we are all aware, harms to children can develop quickly, and it is critical that the approach to priority harms to children is agile and able to respond at pace. The use of secondary legislation will allow the list to be updated to reflect emerging harms without requiring any changes to primary legislation.

Joint Committee Recommendation – Definition of content harmful to children (Para 204):

127. *We recognise the concerns that, without proper guidance, service providers might seek to place disproportionate age assurance measures in place, impacting the rights of both children and adults. We recommend that Ofcom be required to develop a mandatory code of practice for complying with the safety duties in respect of children. Ofcom should be required to have regard to the UN Convention on the Rights of the Child (in particular, General*

Comment No. 25 on children's rights in relation to the digital environment), the Information Commissioner's Office's Age Appropriate Design code, and children's right to receive information under the ECHR when drawing up that code.

Government Response

128. The government supports the aim of this recommendation and recognises the important work that the Age Appropriate Design Code has already done in safeguarding children's personal data. We already expect Ofcom to develop at least one code on complying with the child safety duties. However, it would not be desirable to limit Ofcom's regulatory discretion and risk the effectiveness of the framework with a requirement for only one code of practice for the child safety duties.

129. In terms of writing those codes, Ofcom is already required to consult bodies with expertise in equality issues and human rights when developing codes. We have also amended the Bill to make clear an explicit requirement for consultation with the Information Commissioner, which will ensure that any potential crossovers with data protection regulation aimed at children is considered. The Bill already reflects the principles of the UN Convention on the Rights of the Child General Comment No.25 on children's rights in the digital environment, in particular for the best interests of the child to be a primary consideration; on children's right to life, survival, and development, and; respect for the views of the child. The strongest protections in the Bill are for children. All services subject to the safety duties will need to do far more to protect their users, including children, from illegal content or activity on their services and minimise children's exposure to harmful behaviour. They will also need to support children to have a safe, age-appropriate experience on services that are designed for them.

130. Under the child safety duties, the use of age assurance will be informed by a company's risk assessment and Ofcom's codes of practice. Where Ofcom recommends the use of age assurance it will take into account whether the use is proportionate to the risk. For example, we expect Ofcom to recommend the use of age verification solutions where there is a high level of risk and it is important that services have a high level of confidence in the age of their users, to be able to confidently prevent under-age access to a service. It is not expected that Ofcom will recommend using age verification where the risk level is lower and other measures are considered more appropriate.

131. Services will also have duties to safeguards users' freedom of expression when fulfilling their duties, including their child safety duties. This will further help to safeguard against services implementing solutions that disproportionately prevent children from legitimately accessing a service. In addition, existing data protection legislation requires services to follow the principles of 'lawfulness, fairness and transparency' and 'purpose limitation' when processing users' personal data. This safeguards against services subject to the safety duties implementing age assurance solutions that require disproportionate volumes of personal data and prevents them from using this data in a manner that is incompatible with the original purpose of establishing age.

Joint Committee Recommendation – Alignment with the Age Appropriate Design Code (Para 211):

132. *We recommend that the "likely to be accessed by children'' test in the draft Online Safety Bill should be the same as the test underpinning the Age Appropriate Design Code. This regulatory alignment would simplify compliance for businesses, whilst giving greater clarity to people who use the service, and greater protection to children. We agree that the*

Information Commissioner's Office and Ofcom should issue a Joint Statement on how the two regulatory systems will interact once the Online Safety Bill has been introduced. They should be given powers to cooperate on shared investigations, with appropriate oversight.

Government Response

133. The government considers that the approach taken in the Bill is aligned with the Age Appropriate Design Code and will ensure consistency for businesses. In addition, the status of the legislative test in the Online Safety Bill is binding in a way that the test in the Age Appropriate Design Code is not. As a result, the Bill has a more detailed test to provide greater legal certainty for services, and to enable clearer compliance and effective enforcement of the statutory duties. Ofcom will also be required to consult with the ICO on its guidance to services subject to the safety duties on fulfilling this test which will support the alignment across the Bill and Age Appropriate Design Code.

Joint Committee Recommendation – Pornography (Para 222-223):

134. *Whilst there is a case for specific provisions in the Bill relating to pornography, we feel there is more to be gained by further aligning the Bill with the Age Appropriate Design Code. Whilst we understand the concerns over scope and regulatory burden, this provision would only bring within the scope of the Bill services already covered by the scope of the Age Appropriate Design Code. Both regulatory systems are risk-based and require the regulator to act proportionately. This step would address the specific concern around pornography, requiring all such sites to demonstrate that they have taken appropriate steps to prevent children from accessing their content. It would also bring other sites or services that create a risk of harm into scope whilst bringing us closer to the goal of aligned online regulation across data protection and online safety. We believe that our proposal on expanding the role of risk profiles, discussed later in this report, will be key to ensure that the Bill's provisions impact the riskiest services and are not disproportionate on those at lower risk.*

135. *All statutory requirements on user-to-user services, for both adults and children, should also apply to Internet Society Services likely to be accessed by children, as defined by the Age Appropriate Design Code. This would have many advantages. In particular, it would ensure all pornographic websites would have to prevent children from accessing their content. Many such online services present a threat to children both by allowing them access and by hosting illegal videos of extreme content*

Government Response

136. The government has listened carefully to the feedback on children's access to online pornography since the publication of the draft Bill in May 2021, and in particular to the concerns about pornography on online services not in scope of the Bill. To further strengthen protections for children, we have incorporated a standalone provision into the Bill requiring providers who publish or place pornographic content on their services to prevent children from accessing that content. This addresses the concerns that have been raised about a gap in scope, and ensures that all services that would have been captured by both Part 3 of the Digital Economy Act and all the user-to-user and search services covered by Online Safety Bill will be required to protect children from pornography. This new duty will be enforced by Ofcom with providers being subject to the same enforcement measures as services subject to the safety duties.

137. The Age Appropriate Design Code applies to "information society services" likely to be accessed by children, a definition which derives from the General Data Protection Regulation. "Information society services" are defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'. This

includes many apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet.

138. The new standalone provision on published pornography will apply to any internet service, which we consider covers a comparable or broader range of services than that of an information society service. However, we do not believe that the duties of care for user-to-user and search services in the Bill should be further extended to all information society services. The Online Safety Bill is part of the UK's overall digital regulatory landscape and will deliver protections for children alongside existing regulation. As such, it has been designed to bring into scope user-to-user and search services which pose the greatest risk of harm to users and where there is currently limited regulatory oversight. Including all information society services within the reach of the Bill would expand the scope significantly and risk the effectiveness of the regulatory framework, the scope of which must remain targeted and proportionate for services, to avoid undue regulatory burdens, and to enable Ofcom to effectively enforce its requirements.

Joint Committee Recommendation – Age Assurance (Minimum Standards) Bill (Para 236 & 237):

139. *We recommend that the Bill require Ofcom to establish minimum standards for age assurance technology and governance linked to risk profiles to ensure that third party and provider-designed assurance technologies are privacy-enhancing, rights protecting, and that in commissioning such services providers are restricted in the data for which they can ask. Ofcom should also require that service providers demonstrate to them how they monitor the effectiveness of these systems to ensure that they meet the minimum standards required.*

140. *The government should ask Ofcom to prioritise the development of a mandatory age assurance technology and governance code as a priority ahead of the Bill becoming law and, in doing so, set out risk profiles so that the use of such systems is clearly proportionate to the risk. The code must bear in mind that children have rights to freedom of association, participation, and information, as well as the right to protections. We expect this to be in place within three to six months of the Bill receiving Royal Assent.*

Government Response

141. The Committee's recommendations stress the importance of the use of age assurance being proportionate to the risk that a service presents. We are confident that the Bill ensures that this will be the case. The child safety risk assessment will ensure that services subject to the safety duties identify and consider the risks their service poses to children. Ofcom will set out suitable mitigation measures in its codes of practice. It is expected that this will include the use of age assurance where it is considered appropriate and proportionate to the risk. Ofcom is able to include detail in its codes on the types of age assurance technologies that are best suited to different risk profiles. For example, we expect Ofcom to recommend the use of age verification where there is a high level of risk posed to children. Under the Bill, services subject to the safety duties will be required to keep their risk assessments up-to-date and update them before making a significant change to the design or operation of their service.

142. The Bill also allows Ofcom to set out in its codes of practice the standards services subject to the safety duties could be expected to follow when using age assurance technologies to fulfil their child safety duties. Ofcom can name specific industry standards and principles in its codes of practice, where Ofcom has assessed these will help services to achieve the child safety duties and their wider duties, including on user privacy. These would apply to services subject to the safety duties using either proprietary solutions or third party solutions. Services subject to the safety duties will be required to either follow the steps

set out in the codes of practice, including any standards referenced, in order to be deemed compliant or take alternative steps which demonstrate with (detailed records and explanations) to Ofcom that they have complied with the safety duties.

143. In addition, as part of the new standalone provision for published pornography Ofcom will be required to prepare guidance for pornography providers which must set out the principles that Ofcom will apply when determining compliance with the duties. As with codes of practice, this might include naming specific industry standards, where Ofcom has assessed these will help these services comply with the duty to prevent children from accessing published pornography.

144. We welcome the Committee's interest in the approach being taken to age assurance technologies in the Bill; they are a crucial child safety tool. We look forward to working closely on this area with parliamentarians during the Bill's passage to ensure the legislation delivers appropriate protection for users, especially children.

145. The Committee's recommendation rightly makes reference to the importance of protecting users', specifically child users', privacy and their wider rights. The Bill includes duties on both Ofcom and all services in relation to user privacy. All services will be required to have regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of their service (including, but not limited to, any such provision or rule concerning the processing of personal data) when putting in place measures to protect children – including age assurance. Ofcom will be required to incorporate safeguards for privacy in the codes of practice. In doing so, we expect Ofcom to draw on the expertise of the Information Commissioner's Office; Ofcom will be required to consult with the Information Commissioner on the codes of practice.

146. For the new standalone duty to prevent children encountering published pornographic content, services in scope will be required to keep a written record, in an easily understandable form, of the way in which the provider has had regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of an internet service (including, but not limited to, any such provision or rule concerning the processing of personal data). Ofcom will be required to produce guidance which includes examples of ways in which a provider may have regard to the importance of protecting users' privacy and principles that it proposes to apply when determining whether a provider has complied with this privacy duty. Ofcom will also be required to consult the Information Commissioner on this guidance.

147. The Committee's recommendation regarding the collection of personal data is out of scope of the Bill and is the remit of the Information Commissioner's Office; it is covered in existing data protection legislation, including the Age Appropriate Design Code.

148. The Bill will also ensure users' freedom of expression is safeguarded, this includes access to information. Services subject to the safety duties will have to consider and implement safeguards for freedom of expression when fulfilling their duties. This includes their child safety duties. Ofcom will also need to realise its new duties in a way that protects freedom of expression. In recognition of their size and higher level of risk, including for children, Category 1 services will have additional duties to assess their impact on users' rights and to take steps to mitigate this impact.

Platform design and risk

SUMMARY

- An approach that embeds safety at the design stage of a service is integral to tackling online harms, and will be crucial for a service's compliance with the safety duties. Platform design choices directly impact on the likelihood of harm occurring. Therefore services subject to the safety duties will need to understand, assess and mitigate the risks that their design choices present to users.
- The Joint Committee's recommendations in this area focused on mandating content-neutral safety by design requirements, which it indicates would address the harm caused by disinformation, and on the standard of the risk assessment.
- Ofcom are already carrying out extensive work to begin preparing for the regulatory regime, but some activities will require primary legislation to be passed before they can begin.
- We welcome many of these recommendations where they align with the principles of the Bill and the proportionate and risk-based approach. Since publication of the draft Bill, we have developed the Bill further:
  - At introduction the Bill will require services to produce suitable and sufficient risk assessments and give Ofcom the power to require a company with a substandard risk assessment to take measures to mitigate risks it has missed at the same time as it redoes its risk assessment.
  - The Bill will be amended to require Ofcom to consult with the Information Commissioner as Ofcom forms its risk assessment guidance.

Joint Committee Recommendation – Safety by design as a mitigation measure (Para 82):

149. *We recommend that the Bill includes a specific responsibility on service providers to have in place systems and processes to identify reasonably foreseeable risks of harm arising from the design of their platforms and take proportionate steps to mitigate those risks of harm. The Bill should set out a non-exhaustive list of design features and risks associated with them to provide clarity to service providers and the regulator which could be amended by*

Parliament in response to the development of new technologies. Ofcom should be required to produce a mandatory Safety by Design code of practice, setting out the steps providers will need to take to properly consider and mitigate these risks. We envisage that the risks, features and mitigations might include (but not be limited to):

a. *Risks created by algorithms to create "rabbit holes", with possible mitigations including transparent information about the nature of recommendation algorithms and user control over the priorities they set, measures to introduce diversity of content and approach into recommendations and to allow people to deactivate recommendations from users they have not chosen to engage with;*

b. *Risks created by auto-playing content, mitigated through limits on auto-play and auto-recommendation;*

c. *Risks created by frictionless cross-platform activity, with mitigations including warnings before following a link to another platform and ensuring consistent minimum standards for age assurance;*

d. *Risks created through data collection and the microtargeting of adverts, mitigated through minimum requirements for transparency around the placement and content of such adverts;*

e. *Risks created by virality and the frictionless sharing of content at scale, mitigated by measures to create friction, slow down sharing whilst viral content is moderated, require active moderation in groups over a certain size, limit the number of times content can be shared on a "one click" basis, especially on encrypted platforms, have in place special arrangements during periods of heightened risk (such as elections, major sporting events or terrorist attacks); and*

f. *Risks created by default settings on geolocation, photo identification/sharing and other functionality leading to victims of domestic violence or VAWG being locatable by their abusers, mitigated through default strong privacy settings and accessible guidance to victims of abuse on how to secure their devices and online services.*

Government Response

150. The government agrees that it is vital for services to consider the risks that the features of their service may pose to users. It is helpful that the Committee has highlighted some examples of specific potentially risky functionalities. We are confident that the features listed by the Committee that are within scope of the Online Safety Bill are covered in a future-proofed way by the relevant risk assessment provisions for both Ofcom and services.

151. The risk assessment duties include a requirement to "[take] into account (in particular) algorithms used by the service and how easily, quickly and widely content may be disseminated by means of the service." This captures the Committee's recommendation to include an assessment of risk relating to algorithms and the autoplaying of content. The Committee's concerns about rapid and wide dissemination of content are also captured by this duty.

152. In addition, the definition of "functionality" includes the forwarding or sharing of content with other users; sharing content on other internet services; sharing current or historic location information with other users of the service, recording a user's movements, or identifying which other users of the service are nearby; and accessing other internet services through content present on the service (for example through hyperlinks). This definition therefore captures the Committee's recommendations on sharing viral content, including cross-platform sharing, and the risk created by "default settings on geolocation, photo identification/sharing". Ofcom must take account of these functionalities along with other characteristics of services subject to the safety duties in developing risk profiles.

153. Ofcom's guidance on risk assessments will help services subject to the safety duties to consider the risks presented by these functionalities. Ofcom's codes of practice will set out recommended steps services could take to mitigate these risks as part of their safety duties as part of their illegal content and children's safety duties.

Joint Committee Recommendation – Safety by design as a mitigation measure (Para 83):

154. *We recommend that the Bill includes a requirement for service providers to cooperate to address cross-platform risks and on the regulator to facilitate such cooperation.*

Government Response

155. The government recognises the risks caused by cross-platform activity, and welcomes the Committee's interest in this area. The Bill addresses cross-platform risks in a number of ways. Ofcom's overall risk assessment will cover risks associated with harms moving across different services subject to the safety duties. Services' own risk assessments will also have to consider this. They will have to look at the level of risk of users encountering harmful content by means of their services, not just on the services themselves. They will have to look at risks linked to their services enabling users to share content on other internet services and to access other internet services via content on the service (for example through hyperlinks). They will be obliged to mitigate these risks under their illegal content and children's safety duties.

156. Ofcom's existing information gathering powers will also help to address cross-platform risks. Ofcom will undertake research and horizon-scanning to identify any cross-platform emerging issues, backed up by robust information-gathering powers. This will ensure it has a full picture of the cross-platform nature of harms. Ofcom will also be carrying out work on online safety partnerships that will be beneficial to understanding cross-industry risks, how industry bodies and others bring services together, and facilitating cooperation to address them. In addition, the super-complaints process will enable organisations to submit evidence of systemic issues that are causing harm to certain groups across more than one service.

Joint Committee Recommendation – Societal harm and the role of safety by design (Para 107):

157. *The viral spread of misinformation and disinformation poses a serious threat to societies around the world. Media literacy is not a standalone solution. We have heard how small numbers of people are able to leverage online services' functionality to spread disinformation virally and use recommendation tools to attract people to ever more extreme behaviour. This has resulted in large-scale harm, including deaths from COVID-19, from fake medical cures, and from violence. We recommend content neutral safety by design requirements, set out as minimum standards in mandatory codes of practice. These will be a vital part of tackling regulated content and activity that creates a risk of societal harm, especially the spread of disinformation. For example, we heard that a simple change, introducing more friction into sharing on Facebook, would have the same effect on the spread of mis- and disinformation as the entire third-party fact checking system.*

Government Response

158. The government shares the Committee's concern on the impact of dangerous misinformation and disinformation. The Bill will require all services subject to the safety duties to remove harmful misinformation and disinformation where it is illegal content in scope of the Bill. This includes services which are likely to be accessed by children which will also need to

take steps to protect children from misinformation and disinformation which could be harmful to them. Category 1 services will also have to address categories of priority content which are legal but could cause harm to individual adults. Priority categories of legal but harmful content will cover some types of harmful misinformation and disinformation such as anti-vaccination and other health misinformation that poses a threat to public health.

159. Ofcom, in its codes of practice, will set out the steps services subject to the safety duties can take to mitigate these risks. These steps will include, where appropriate, design choices or interventions, which would by their nature be content neutral. The steps services will be expected to take would be proportionate to the risk presented by the service. Ofcom will also be required to set up an advisory committee on misinformation and disinformation to build understanding of this issue, which may consider the issue of societal harms.

160. Additionally, the government is taking a range of non-legislative measures to tackle this issue. This includes standing up the Counter Disinformation Unit during periods of heightened vulnerability such as elections or the COVID-19 pandemic. The Unit provides a picture of the extent, scope and the reach of dangerous misinformation and disinformation and works with partners to identify and respond to it in line with platform terms and conditions. The government is also building audience resilience to misinformation and disinformation through media literacy initiatives, working collaboratively with international partners, and undertaking a wide-ranging programme of research to understand the scale, scope, and impact of online manipulation.

161. This approach will tackle a significant amount of harm arising from misinformation and disinformation. We believe the approach described above addresses the issues raised by the Committee's recommendation. Binding minimum standards would not be possible nor would it provide a proportionate or risk-based approach given the range of services in scope.

Joint Committee Recommendation – Naming the risk assessments (Para 317):

162. *To help differentiate between the risk assessment undertaken by the regulator and that undertaken by the service providers, Ofcom's risk assessment should be renamed the "Ofcom register of risks of regulated services" (henceforth, register of risks). Ofcom should begin working on this immediately so that it is ready to be actioned when the Bill becomes law.*

Government Response

163. We thank the Joint Committee for this recommendation and have ensured clarity by renaming Ofcom's assessments as "Ofcom's Register of Risks of Part 3 services." Ofcom is already carrying out extensive work to begin preparing for the new regulatory regime, but not activities that require primary legislation to be passed.

Joint Committee Recommendation – Establishing risk profiles for companies of different kinds (Para 323):

164. *The Bill's provision that Ofcom should develop risk profiles based on the characteristics of services should be strengthened. Ofcom should begin drawing up risk profiles immediately so that they are ready to be actioned when the Bill becomes law. Risk profiles should reflect differences in the characteristics of the service. These could include (but are not limited to) risks created by algorithms; risks created by a reliance on artificial intelligence moderation; risks created by unlimited 'one-click' sharing; risks caused by "engagement" maximising design features; risk of unsupervised contact between adults and children which may give rise to grooming; risks caused by surveillance advertising; and such other risks as Ofcom*

identifiers in its overall risk assessment, as well as platform design, risk level, end-to-end encryption, algorithmic design, safety by design measures, and the service's business model and overall corporate aim. Ofcom should also be able to take into account whether a company has been the subject of a super complaint, other legal proceedings or publicly documented evidence of poor performance e.g. independent research, a poor monitoring report in the EU's code of Conduct for Illegal Hate, or whistleblowers' evidence.

Government Response

165. As well as risk levels and other matters they identify in their risk assessment, Ofcom must also consider the functionalities of services subject to the safety duties which are defined in detail in the Bill, and other systems and processes when developing risk profiles. Ofcom will be able to take account of all relevant evidence in assessing risk levels when preparing their guidance, which could include evidence that comes from super-complaints or legal proceedings.

166. Although Ofcom is already carrying out extensive work to begin preparing for the regulatory regime, some activities will require primary legislation to be passed before they can begin. For example, Ofcom may need statutory information gathering powers to obtain the evidence needed to finalise proposals for consultation, or to issue requests during consultation periods. It will be important for there to be certainty about what the legislation will require before Ofcom consults on how new functions will be exercised. Any consultation will need to reflect the final legal position and allow consultees to be able to provide fully informed responses.

Joint Committee Recommendation – Establishing minimum quality standards for risk assessments (Para 332-333):

167. *It should not be possible for a service provider to underestimate the level of risk on their service without fear of sanction. If Ofcom suspects such a breach it should have the power to investigate and, if necessary, to take swift action. We are not convinced that the draft Bill as it currently stands achieves this.*

168. *Ofcom should be required to set binding minimum standards for the accuracy and completeness of risk assessments. Ofcom must be able to require a provider who returns a poor or incomplete risk assessment to redo that risk assessment. Risk assessments should be carried out by service providers as a response to the Online Safety Act before new products and services are rolled out, during the design process of new features, and kept up to date as they are implemented.*

Government Response

169. We agree with the Committee that it is important that services' risk assessments do not underestimate the level of risk on their service. Upon redrafting, the Bill will state that services subject to the safety duties' risk assessments must be 'suitable and sufficient', making it clearer that enforcement will be available against a substandard risk assessment. It will also enable Ofcom to require a company with a substandard risk assessment to take measures to mitigate the risks it has missed, at the same time as it redoes its risk assessment. We also agree that it is important for services to consider the potential risks of changes to the services, review implementation, and to keep their risk assessments up to date, and this is already required by the Bill.

170. However, we do not believe that the approach recommended by the Committee of setting binding minimum standards would be appropriate or effective. It would be very challenging to make these proportionate across the range of services subject to the safety duties and would not be future proofed, as risk will evolve. It would also have the potential

to drive compliance to a minimum common denominator, rather than expecting more of major services. We assess that our approach will meet the same objective in preventing substandard risk assessments.

Joint Committee Recommendation – Establishing minimum quality standards for risk assessments (Para 334):

171. *The required content of service providers' risk assessments should follow the risk profiles developed by Ofcom, which in turn should be based on the differences in the characteristics of the service, platform design, risk level, and the service's business model and overall corporate aim. For example, a provider that does not have an engagement based service would not need to address irrelevant risks associated with virality, whilst a site containing adult content would have to address the higher level of risks associated with children accessing the site.*

Government Response

172. The government agrees that the factors listed by the Joint Committee are important aspects of services subject to the safety duties' risk assessments and should be considered in a proportionate way. This recommendation is already covered by the Bill through requiring services subject to the safety duties to take into account the relevant risk profiles and guidance as well as the matters set out in the Bill when undertaking their own risk assessments.

Joint Committee Recommendation – Establishing minimum quality standards for risk assessments (Para 335):

173. *The Bill should be amended to clarify that risk assessments should be directed to "reasonably foreseeable" risks, to allow Ofcom greater leeway to take enforcement action against a company that conducts an inadequate risk assessment.*

Government Response

174. We welcome the aim of this recommendation, which will be addressed by drafting changes to the Bill to ensure that services' risk assessments must be 'suitable and sufficient'. This will enable enforcement against a poor or incomplete risk assessment. As set out above, Ofcom will also be able to require a company with a substandard risk assessment to take measures to mitigate risks it has missed at the same time as it redoes its risk assessment. We therefore do not consider it necessary to require services' to include 'reasonably foreseeable' risks in their RAs, as the Joint Committee's concerns will be addressed through the changes we are making.

Joint Committee Recommendation – Establishing minimum quality standards for risk assessments (Para 336):

175. *Ofcom should look to the Data Protection Impact Assessment as they come to form their own guidance for minimum standards for risk assessments for regulated services.*

Government Response

176. The government supports this recommendation. We have amended the Bill to require Ofcom to consult with the ICO (who are responsible for Data Protection Impact Assessments), as Ofcom forms its risk assessment guidance. This will achieve the recommendation's aims.

Powers of the regulator

SUMMARY

- This chapter considers the powers that the Bill will confer on Ofcom, to allow it to carry out its online safety functions.
- The Joint Committee's recommendations in this area focused on a number of the powers that the Bill will confer on Ofcom. This includes strengthening Ofcom's audit and information gathering powers to ensure that Ofcom has a suite of powers that match those of similar regulators and commencement of the senior manager liability provisions. This section also focussed on the Secretary of State's powers, media literacy initiatives and use of technology warning notices.
- Since publication of the draft Bill, we have developed the Bill further to:
  - Provide Ofcom with audit powers;
  - Commence the senior manager liability offence as soon as possible after Royal Assent; and
  - Made a number of changes to the use of technology power.
- Both government and Ofcom recognise the importance of moving as quickly as possible to launch the regime once the Online Safety Bill has passed. As a result, Ofcom is already taking a range of preparatory steps, such as conducting research into the nature, prevalence and impact of online harms and the options for mitigating these harms.
- Doing this research now will not only help Ofcom establish itself as a global thought leader on online harms issues but will also enable it to build the evidence base needed to start consulting on key elements of the regime such as codes of practice and risk assessment as soon as practicably possible after Royal Assent.

Joint Committee Recommendation – Powers of audit (Para 339):

177. *In bringing forward the final Bill, we recommend the government publish an assessment of the audit powers given to Ofcom and a comparison to those held by the Information Commissioner's Office and the Financial Conduct Authority. Parliament should be reassured*

that the Bill will give Ofcom a suite of powers to match those of similar regulators. Within six months of the Act becoming law Ofcom should report to Parliament on how it has used those powers.

Government Response

178. The Bill sets out a suite of robust information powers for Ofcom. These powers are based on powers which have worked effectively in other regulatory regimes and will allow Ofcom to properly assess whether all services are fulfilling their duties. As part of this suite of powers, Ofcom will have the power to require a company to undergo, and pay for, a skilled person's report which could be used to assess potential non-compliance, and/or to build Ofcom's understanding of the risks associated with the operation of a provider's service. Ofcom will also have powers to enter and inspect premises, documentation, and equipment. In light of the Committee's recommendation, we have amended the wording of the redrafted Bill to make explicit that Ofcom will have the power to undertake audits. This will ensure that Ofcom's information powers are at least equivalent to the ICO's powers and will enable Ofcom to assess compliance and risk, effectively. We do not consider it necessary to publish an assessment of the audit powers given to Ofcom. Therefore, we will not be taking forward this recommendation. In addition, we do not judge that a change to the Bill is needed for Ofcom to report to Parliament on the use of its powers, as it can do so via its annual report.

Joint Committee Recommendation – Powers of audit (Para 340):

179. *We recommend that the largest and highest-risk providers should be placed under a statutory responsibility to commission annual, independent third-party audits of the effects of their algorithms, and of their risk assessments and transparency reports. Ofcom should be given the explicit power to review these and undertake its own audit of these or any other regulated service when it feels it is required. Ofcom should develop a framework for the effective regulation of algorithms based on the requirement for, and auditing of, risk assessments.*

Government Response

180. During scrutiny, the stakeholder evidence on this point served to underscore why Ofcom has been given robust information and investigation powers in the Bill. As mentioned above, the updated draft Bill will allow Ofcom to undertake audits of companies, where necessary. The Bill also recognises the value of independent third party assessments, which is why Ofcom will have the power to require skilled person reports. This will allow Ofcom to require reports by expert third parties. Ofcom will be able to use these powers to help understand whether services are addressing the risk of harm associated with their algorithms and to assess whether these services are meeting their risk assessment and transparency duties.

Joint Committee Recommendation – Criminal liability (Para 367):

181. *The Bill should require that companies' risk assessments be reported at Board level, to ensure that senior management know and can be held accountable for the risks present on the service, and the actions being taken to mitigate those risks.*

Government Response

182. The government agrees with the Joint Committee that senior level engagement in a service's risk assessment and management processes will be important. We expect Ofcom will consider including measures on senior level engagement in its codes of practice and/

or guidance on risk assessments, including setting out what types of measures would be appropriate for different size services. Therefore, we do not think specific provisions on reporting at Board level are needed within the Bill.

Joint Committee Recommendation – Criminal liability (Para 368):

183. *We recommend that a senior manager at board level or reporting to the board should be designated the "Safety Controller'' and made liable for a new offence: the failure to comply with their obligations as regulated service providers when there is clear evidence of repeated and systemic failings that result in a significant risk of serious harm to users. We believe that this would be a proportionate last resort for the Regulator. Like any offence, it should only be initiated and provable at the end of an exhaustive legal process.*

Government Response

184. As above, we expect Ofcom will consider including in its codes and/or guidance the measures on senior level engagement that it expects services subject to the safety duties to take, proportionate to their size and type of service. This may include having a senior person designated as responsible for certain aspects of the Online Safety regime, if appropriate and proportionate.

185. Senior level engagement will be important to the success of the regime. The Bill includes a criminal offence for senior managers (which we discuss further below), should they fail to ensure their service complies with Ofcom's information requests. We have targeted senior management liability in this area as it is crucial that Ofcom has the information it needs to successfully regulate the sector. We believe this offence – within the full suite of enforcement powers – will push strong compliance with the regime. We are therefore not proposing to introduce additional criminal offences for senior managers, and do not believe that it would be proportionate to do so.

Joint Committee Recommendation – Criminal liability (Para 369):

186. *The Committee welcomes the Secretary of State's commitment to introduce criminal liability within three to six months of Royal Assent and strongly recommends that criminal sanctions for failures to comply with information notices are introduced within three months of Royal Assent.*

Government Response

187. The Secretary of State confirmed her intention to the Joint Committee to ensure Ofcom has this power available as quickly as possible. While the senior manager's offence was previously intended to be commenced after a post-legislative review at least two years after Royal Assent, we are now bringing the offence forward to commence as soon as possible after Royal Assent.

188. Tech company executives must take these new laws seriously. The framework has been designed to change the conversation in the boardroom from only thinking about the bottom line to thinking seriously about user safety. The senior managers' offence in the Bill will help push strong engagement with the regime and hold tech executives to account.

Joint Committee Recommendation – Secretary of State powers (Para 377):

189. *The powers for the Secretary of State to a) modify codes of practice to reflect government policy and b) give guidance to Ofcom give too much power to interfere in Ofcom's independence and should be removed.*

Government Response

190. 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 public policy. For example, if Ministers thought that a code could have an adverse economic or public policy impact.

191. 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 to develop or update a code, rather than at any stage, and the details of any direction given would be published alongside the modified code.

192. 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. Ofcom must have regard to guidance issued by the Secretary of State, but is not bound by it. The guidance is intended to be used to publicly set out the government's strategic expectations of how Ofcom will exercise its statutory functions, where deemed necessary, in order to provide more certainty of the government's intentions to both Ofcom and businesses.

Joint Committee Recommendation – Secretary of State powers (Para 378):

193. *Exercise of the Secretary of State's powers in respect of national security and public safety in respect of terrorism and child sexual exploitation and abuse content should be subject to review by the Joint Committee we propose later in this report.*

Government Response

194. We are considering the best way to provide post-legislative scrutiny of the Online Safety Act in a way which makes the most of the skills and expertise in both Houses. We do not, however, intend to bring in a standing Joint Committee through primary legislation and give that committee statutory powers, including in respect of the Secretary of State's powers in relation to national security and public safety.

Joint Committee Recommendation – Minimum standards for media literacy initiatives (Para 381-382):

195. *If the government wishes to improve the UK's media literacy to reduce online harms, there must be provisions in the Bill to ensure media literacy initiatives are of a high standard. The Bill should empower Ofcom to set minimum standards for media literacy initiatives that both guide providers and ensure the information they are disseminating aligns with the goal of reducing online harm.*

196. *We recommend that Ofcom is made responsible for setting minimum standards for media literacy initiatives. Clause 103 (4) should be amended to include "(d) about minimum standards that media literacy initiatives must meet."*

Government Response

197. Ofcom has recently published a new approach to online media literacy, which expands significantly on its current activity. Ofcom began this new work programme before the passage of the Bill, highlighting that the powers under its existing duty in section 11 of the Communications Act are sufficient. Clause 103 of the draft Bill clarified Ofcom's duties with regard to media literacy, but did not grant Ofcom any additional powers. As such, it is clear that including the media literacy clause from the draft Bill (clause 103) would create unnecessary regulation. It has therefore been removed. Ofcom retains its existing media literacy duties under the Communications Act and is able to deliver the responsibilities that were previously set out in Clause 103.

198. We agree with the sentiment of this recommendation that work should be undertaken to ensure media literacy initiatives are of a high quality. However, as Clause 103 has been removed from the Bill, we think it is best addressed through non-legislative means. We are committed to working with Ofcom to explore ways of ensuring high quality initiatives that address all aspects of media literacy. Ofcom's forthcoming work on evaluation will be particularly important in this regard.

Joint Committee Recommendation – Ofcom's duty to improve media literacy (Para 385):

199. *We recommend that the Bill reflects that media literacy should be subject to a "whole of government" approach, involving current and future initiatives of the Department of Education in relation to the school curriculum as well as Ofcom and service providers. We have heard throughout this inquiry about the real dangers that some online content and activity poses to children. Ofsted already assesses how schools manage online safety as part of their safeguarding policies. We recommend that Ofsted, in conjunction with Ofcom, update the school inspection framework to extend the safeguarding duties of schools to include making reasonable efforts to educate children to be safe online.*

Government Response

200. We are committed to working together with all stakeholders across government to improve media literacy throughout the UK. This recommendation does not refer specifically to changes that can be made to the Bill. However, we are, and have plans to continue, undertaking non-legislative measures to bring together other government stakeholders to work towards the objectives outlined in this recommendation.

201. This includes working closely with the Department for Education to consider what more the government can do to improve media literacy education in schools and other formal education settings. We also regularly engage with Ofcom to coordinate work and share best practice. We will discuss with Ofcom options for engaging with Ofsted.

Joint Committee Recommendation – Ofcom's duty to improve media literacy (Para 386):

202. *Ofcom should require that media literacy is built into risk assessments as a mitigation measure and require service providers to provide evidence of taking this mitigation measure where relevant.*

Government Response

203. The government agrees that media literacy is an important tool for service providers to use in the mitigation of risk to users. We are taking forward this recommendation by including a category in the risk assessment duties for services to consider how the design and operation of a service can be used to promote media literacy, as a means of risk mitigation.

204. Additionally, we plan to work with Ofcom to explore ensuring service providers are utilising design features that encourage media literacy to support the online safety of their users. Ofcom's recently published 'approach to online media literacy' document sets out plans to do this, including establishing a working group to explore the role of online platforms in promoting media literacy.

205. The government's Online Media Literacy Strategy, launched in July 2021, also sets out plans to support organisations to empower users to make safer choices online and mitigate harms. This includes exploring the role of platform design in promoting media literacy, and setting direction for actions we want to see online platforms take.

Joint Committee Recommendation – Media literacy and a focus on individual rather than societal harms (Para 388):

206. *We recommend that Clause 103(11) is amended to state that Ofcom's media literacy duties relate to "the public" rather than "members of the public", and that the definition of media literacy is updated to incorporate learning about being a good digital citizen and about platform design, data collection and the business models and operation of digital services more broadly.*

Government Response

207. As outlined in the above responses to recommendations, the draft Bill's Clause 103 has been removed from the draft Bill. The first part of this recommendation relating to the wording 'members of the public' will be achieved by removing Clause 103 and reverting to the original wording of Ofcom's media literacy duty in Section 11 of the 2003 Communications Act.

208. Alongside the Bill, we are undertaking a suite of non-legislative media literacy activity as set out in our Online Media Literacy Strategy. Our approach takes a broad definition of media literacy, including the points set out in this recommendation, and allows for a broad spectrum of activity.

Joint Committee Recommendation – Use of technology warning notices (Para 394):

209. *The highest risk services, as assessed by Ofcom, should have to report quarterly data to Ofcom on the results of the tools, rules, and systems they have deployed to prevent and remove child sexual exploitation and abuse content (e.g. number and rates of illegal images blocked at upload stage, number and rates of abusive livestreams terminated, number and rates of first- and second-generation images and videos detected and removed).*

Government Response

210. The issue of Child Sexual Exploitation & Abuse (CSEA) online is a critical one. Ofcom's existing powers will allow it to require services subject to the safety duties to provide information on the effectiveness of their systems and processes on a regular basis, and as such, we are not going to make this a statutory requirement in the Bill, as this would be at odds with the rest of the framework, which already allows Ofcom to require any necessary and appropriate information from a regulated service by notification.

211. Further analysis of volume and trends may be possible through data received as part of the new CSEA reporting requirement. In response to the government's commitment to tackling CSEA, the Online Safety Bill will require in-scope companies to go further than the duties of care by introducing a requirement to report CSEA detected on their platforms to the National Crime Agency.

212. 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.

213. In-scope companies will need to demonstrate existing reporting obligations to be exempt from this requirement, which will avoid duplication of companies' efforts. Ofcom may request information about a company's reporting and will have access to the full suite of enforcement options for non-compliance.

Joint Committee Recommendation – Use of technology warning notices (Para 395 & 396):

214. *Ofcom should have the power to request research and independent evaluation into services where it believes the risk factors for child sexual exploitation and abuse are high.*

215. *Ofcom should move towards a risk factors approach to the regulation of child sexual exploitation and abuse material. It should be able to issue a Use of Technology notice if it believes that there is a serious risk of harm from child sexual exploitation and abuse or terrorism content and that not enough is being done by a service to mitigate those risks. The Bill should be amended to clarify that Ofcom is able to consider a wider range of risk factors when deciding whether to issue a Use of Technology notice or take enforcement action. Risk factors should include:.*

a. *The prevalence or the persistent prevalence of child sexual exploitation and abuse material on a service, or distributed by a service;*

b. *A service's failure to provide and maintain adequate tools, rules, and systems to proactively prevent the spread of child sexual exploitation and abuse content, and to provide information on those tools, rules, and systems to Ofcom when requested;*

c. *A service's failure to provide adequate data to Ofcom on the results of those tools, rules, and systems (e.g., number and rates of illegal images blocked at upload stage, number and rates of abusive livestreams terminated, number and rates of first- and second-generation images and videos detected and removed);*

d. *The nature of a service and its functionalities;*

e. *The user base of a service;*

f. *The risk of harm to UK individuals (and the severity of that harm) if the relevant technology is not used by the service;*

g. *The degree of interference posed by the use of the relevant technology with users' rights to freedom of expression and privacy; and*

h. *The safety by design mechanisms that have been implemented.*

Government Response

216. In terms of the proposed changes to the use of technology warning notices, we agree that Ofcom must be able to use this power effectively to address terrorism and child sexual exploitation and abuse (CSEA), when it is justified.

217. With regards to the first recommendation on requesting research and independent evaluation, Ofcom will already be able to require information from services, through its information gathering. Equally, we expect that Ofcom will also conduct research into the wider risk landscape. We therefore do not think any further changes are needed.

218. On the second recommendation, the government agrees that a change is required to the basis on which a Use of Technology Notice can be issued. As such, we have amended this power to enable Ofcom to take a more risk-based approach to doing so. The requirement for Ofcom to have evidence of 'persistent' and 'prevalent' harm on services before it can issue a notice has been removed. It has been replaced with a requirement for Ofcom to demonstrate that the use of the power is justifiable because it is necessary and proportionate to the risk of harm with regard to the anticipated level of interference of user's rights to privacy and freedom of expression. Ofcom must take into account certain supporting criteria when evidencing this decision. This will give Ofcom greater flexibility in deciding whether it is able to take action under the Use of Technology provisions, and will provide a transparency to its decision making.

219. The criteria will be included in primary legislation and require Ofcom to consider a range of factors when making this decision, including the risk of harm occurring on a service and evidence of harm. This approach will allow Ofcom to draw on a wider range of evidence than they would have done under the 'persistent and prevalent' safeguard in the draft of the Bill.

220. In addition, we have made the power available to Ofcom as a stand alone power; the exercise of the power is no longer dependent on the service having breached the safety duty. This means that even if a service has followed the codes of practice in relation to the safety duty and there is still CSEA content on its platform, Ofcom may issue a notice.

Joint Committee Recommendation – The regulation of child sexual exploitation and abuse material (Para 353):

221. *Ofcom may receive unsolicited child sexual exploitation and abuse material which would constitute an offence under Section 1 of the Protection of Children Act 1978. The Bill should be amended to provide Ofcom with a specific defence in law to allow it to perform its duties in this area without inadvertently committing an offence.*

Government Response

222. We agree it is critical that Ofcom be able to regulate without being concerned about the prosecution of its staff and, as such, a provision to this effect has been included in the revised Bill.

Regulatory cooperation & Parliamentary oversight

SUMMARY

- This chapter covers the way in which Ofcom, as the online safety regulator, will work with other regulators with an interest in the online space, and how Parliament will oversee the framework's operation.
- The Joint Committee's recommendations in this area focused on ensuring that there are statutory routes to ensure cooperation between regulators, and for Parliament to scrutinise their functions and activities. The Committee further recommended a change to ensure whistleblowers who report safety risks to the regulator are protected.
- Since publication of the draft Bill, we have developed the Bill further to:
  - Introduce an information sharing gateway, giving Ofcom the ability to share information with international regulators.
  - Introduced references on the face of the Bill to the Information Commissioner as a statutory consultee on issues relating to privacy.
- Amendments will also be made to the Public Interest Disclosure (Prescribed Persons) Order 2014 as a result of the Joint Committee's recommendations, to ensure whistleblowers who report information on online safety breaches to Ofcom are protected.

Joint Committee Recommendation – Coregulation (Para 346 – 347):

223. *In taking on its responsibilities under the Bill, Ofcom will be working with a network of other regulators and third parties already working in the digital world. We recommend that the Bill provide a framework for how these bodies will work together including when and how they will share powers, take joint action, and conduct joint investigations.*

224. *We reiterate the recommendations by the House of Lords Communications and Digital Committee in their Digital Regulation report: that regulators in the Digital Regulation Cooperation Forum should be under a statutory requirement to cooperate and consult with one another, such that they must respect one another's objectives, share information, share powers, take joint action, and conduct joint investigations; and that to further support*

coordination and cooperation between digital regulators including Ofcom, the Digital Regulation Cooperation Forum should be placed on a statutory footing with the power to resolve conflicts by directing its members.

Government Response

225. Per the government's answer on international collaboration, the redrafted Bill will include a new information sharing gateway, which will enable Ofcom to share information with other regulators internationally in addition to the existing provisions for sharing information with domestic regulators.

226. With regards to the Digital Regulation Cooperation Forum (DRCF), as part of the government's Plan for Digital Regulation, we have been considering how to improve coordination between digital regulators. The Digital Regulation Cooperation Forum has shared proposals for statutory coordination mechanisms, including duties to consult/cooperate and new information sharing mechanisms. We have also consulted on potential coordination mechanisms to support the delivery of the forthcoming pro-competition regime and reformed data protection regime, and are considering our responses to these consultations. We will add the Information Commissioner as a statutory consultee for Ofcom's draft codes of practice and relevant pieces of guidance, to ensure that Ofcom benefits from the ICO's expertise, especially around privacy.

227. As set out in our evidence to the Lords Communication and Digital Committee, we do not support the idea of establishing a statutory coordination body. We are concerned that such a body would unnecessarily complicate the regulatory landscape, and confuse issues of regulatory independence and accountability. The DRCF's member regulators are already accountable for their activities through their individual statutory remits, and putting the DCRF on a statutory footing risks duplicating or creating confusion with the individual legislative frameworks. We have provided further clarification on this as part of our response to the Lords Communications and Digital Committee.

Joint Committee Recommendation – Coregulation (Para 348):

228. *The draft Bill does not give Ofcom co-designatory powers. Ofcom is confident that it will be able to co-designate through other means. The government must ensure that Ofcom has the power to co-designate efficiently and effectively, and if it does not, this power should be established on the face of the Bill.*

Government Response

229. Ofcom already has the power to co-designate other bodies to carry out separate functions by virtue of Section 69 of the Deregulation and Contracting Out Act 1994, and Section 1(7) of the Communications Act 2003. We are satisfied that these powers are sufficient, should other bodies be required to deliver aspects of the regime. As such, we do not see a need to amend the Online Safety Bill.

Joint Committee Recommendation – International co-operation (Para 315):

230. *Ofcom should have the power on the face of the Bill to share information and to cooperate with international regulators at its discretion.*

Government Response

231. We agree with the importance of Ofcom being able to share information and cooperate with international regulators. We welcome the recommendation from the Committee and have added provisions on the face of the Bill to do just that. Through the creation of a new information sharing gateway, Ofcom will have the power to share information with regulators internationally. This will help ensure that Ofcom can collaborate effectively with international partners, and promote compliance with the Online Safety Bill.

232. The government also agrees that international collaboration is important in tackling online harms. We continue to engage with international partners to learn from their experiences and build consensus around shared approaches to tackling online harms that uphold our democratic values and promote a free, open and secure internet.

Joint Committee Recommendation – Protections for whistleblowers (Para 439):

233. *We recommend that whistleblowers' disclosure of information to Ofcom and/or the Joint Committee on Digital Regulation, where that information provides clear evidence of non-compliance with the Online Safety Bill, is protected under UK law.*

Government Response

234. We thank the Committee for their consideration of this issue – the government agrees. This will be done separately from the Bill, via a change to the Public Interest Disclosure (Prescribed Persons) Order 2014 to ensure that Ofcom can receive whistleblowers' reports relating to Ofcom's existing video sharing platform regime, and the future online safety regime.

Joint Committee Recommendation – Role and value of a Joint Committee on Digital Regulation (Para 434 – 436):

235. *We agree with other Committees that it is imperative that digital regulation be subject to dedicated parliamentary oversight. To achieve this, we recommend a Joint Committee of both Houses to oversee digital regulation with five primary functions: scrutinising digital regulators and overseeing the regulatory landscape, including the Digital Regulation Cooperation Forum; scrutinising the Secretary of State's work into digital regulation; reviewing the codes of practice laid by Ofcom any legislation relevant to digital regulation (including secondary legislation under the Online Safety Act); considering any relevant new developments such as the creation of new technologies and the publication of independent research or whistleblower testimonies; and helping to generate solutions to ongoing issues in digital regulation.*

236. *We fully support the recommendation of the House of Lords Communications and Digital Committee in their report on Digital Regulation that, as soon as possible, full Digital Regulation Cooperation Forum membership should be extended to statutory regulators with significant interests and expertise in the digital sphere, and that partial membership should be extended to non-statutory regulators and advisory bodies with subject specific knowledge to participate on issues particular to their remits.*

237. *We recommend that, in addition to any other reports the Committee chooses to make, the Joint Committee produces an annual report with recommendations on what could or should change, looking towards future developments. We anticipate that the Joint Committee will want to look at the definition of disinformation and what more can be done to tackle it at an early stage.*

Government Response

238. 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 Joint Committee on the Online Safety Bill, as well as the DCMS Select Committee, its Sub-Committee on Online Harms and Disinformation, and the Lords Communications and Digital Committee.

239. Post-legislative scrutiny of the legislation will provide reassurance the online safety regulatory regime is having the impact we envisage. This is a groundbreaking regulatory framework, relevant to millions of people across the UK and with services from across the globe required to act, including some of the 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.

240. The depth of expertise in both Houses has been an effective way to scrutinise the Bill. 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. The government is not intending to legislate for a new committee via the Online Safety Bill.

241. We note the recommendation from both this Joint Committee and the Lords Communications and Digital Committee, that a Joint Committee on digital regulation should be established. However, 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 recommendation.

242. We note the Committee's recommendation that DRCF's membership be expanded to include other statutory regulators and advisory bodies with relevant interests. As a voluntary, non-statutory cooperation forum, it is ultimately for the DRCF itself to make decisions about its membership. However, as set out in our recent evidence to the Lords Communications and Digital Committee, we agree on the importance of the DRCF engaging with other regulators and bodies with relevant interests in the regulation of digital technologies and are encouraged to see the early steps the DRCF have already taken in this respect. Ultimately, we recognise that there is a trade-off between the breadth and depth of the DRCF's activities. We believe expanding its membership to include all regulators with a role in digital could undermine the DRCF's agility and ability to focus in depth on specific priorities. We welcome the DRCF's views on how they can best strike this balance and ensure that collaboration is targeted appropriately.

Journalism & content of democratic importance

SUMMARY

- This chapter considers how the Bill protects freedom of expression, particularly in those areas where certain types of speech may merit additional protections, on the basis of their wider societal value.
- The Joint Committee's recommendations in this area focused on preventing social media companies from moderating or removing content produced by recognised media organisations, unless that content breaks the law. The Committee also suggests widening the existing protections in the Bill to cover all speech with a public interest, and requiring Ofcom to regularly report on the impact that regulated services have on media plurality.
- We do not agree with the Committee's recommendations in this area. Preventing any moderation of content that meets the definition of news publisher could undermine the overall safety objectives of the Bill. It could require services to retain extreme or violent material that is harmful to their specific users, even if that content breaches their terms and conditions.

Joint Committee Recommendation – Protecting high value speech (Para 304 & 305):

243. *We recommend that the news publisher content exemption is strengthened to include a requirement that news publisher content should not be moderated, restricted or removed unless it is content the publication of which clearly constitutes a criminal offence, or which has been found to be unlawful by order of a court within the appropriate jurisdiction.*

244. *We recommend that the government look at how bad actors can be excluded from the concept of news publishers. We suggest that they may wish to exclude those that have been repeatedly found to be in breach of The Ofcom Broadcasting code, or are publications owned by foreign governments. Ofcom should also examine the use of new or existing registers of publishers. We are concerned that some consumer and business magazines, and academic journals, may not be covered by the Clause 40 exemptions. We recommend that the Department consult with the relevant industry bodies to see how the exemption might be amended to cover this, without creating loopholes in the legislation.*

Government Response

245. The government is committed to defending the invaluable role of a free media, and there are already significant protections for journalistic content in the regulatory framework. Content published by a news publisher on its own site (e.g. on a newspaper or broadcaster's website) will not be in scope of the safety duties, and user comments on that content will be exempted.

246. We agree with the Committee that the Bill also includes strong protections for journalistic content.

247. Firstly, news publishers' content will be exempted from being subject to the safety duties'. These services will be under no legal obligation to apply their new safety duties to such content. This means services subject to the safety duties will not be incentivised to remove news publishers' content as a result of a fear of sanction by Ofcom.

248. There is also a positive obligation on Category 1 services to safeguard journalistic content shared on their services. This includes news publisher content generated for the purposes of journalism. Category 1 services are required to operate a service using systems and processes that ensure that importance of the free expression of journalistic content is taken into account when making decisions on how to treat such content. In doing so, they must offer a higher level of consideration for journalistic content when making content moderation decisions, and must enforce these consistently. In addition, Category 1 services must also offer an expedited route of appeal for journalistic content when it is removed. All other services subject to the safety duties will also need to consider and implement safeguards for freedom of expression when fulfilling their duties.

249. Under the Joint Committee's recommendations, Category 1 services could be required to carry, on a permanent basis,objectionable content produced by more fringe 'news publishers'. However, narrowing the definition of 'recognised news publisher' to mitigate this presents a serious risk of undermining the government's commitment to self-regulation of the press and wider media freedom. The Committee's suggestion to consider new or existing registers of publishers to exclude 'bad actors' would result in the government, Ofcom, or a trade body effectively maintaining a list of 'acceptable' news publishers. We do not intend to take this forward. In defining our existing exemption for recognised news publishers we have already worked to exclude bad actors, for example entities proscribed under the Terrorism Act 2000 and entities whose purpose is to support such organisations.

Joint Committee Recommendation – Protecting high value speech (Para 307):

250. *We recommend that the existing protections around journalistic content and content of democratic importance should be replaced by a single statutory requirement to have proportionate systems and processes to protect 'content where there are reasonable grounds to believe it will be in the public interest'. Examples of content that would be likely to be in the public interest would be journalistic content, contributions to political or societal debate and whistleblowing. Ofcom should produce a binding code of practice on steps to be taken to protect such content and guidance on what is likely to be in the public interest, based on their existing experience and case law. This should include guidance on how appeals can be swiftly and fairly considered. Ofcom should provide guidance to companies in cases of systemic, unjustified take down of content that is likely to be in the public interest. This would amount to a failure to safeguard freedom of expression as required by the objectives of the legislation.*

Government Response

251. We thank the Committee for their consideration of these issues so critical to the regulatory framework. However, the government does not judge that a single statutory requirement is the best way forward. We do not agree with using the term "public interest" as it has a specific meaning, and we do not agree that services subject to the safety duties, which are private companies, are well placed to determine what is in the public interest.

252. Both journalistic content and content of democratic importance have specific, tailored protections which will better safeguard this type of content. The journalistic protections are explained in the answers above. In terms of content of democratic importance, Category 1 services must balance their content moderation objectives with protecting users' access to such content, offering a higher level of consideration for that content when making content moderation decisions.

Joint Committee Recommendation – Competition and media plurality (Para 291):

253. *We recommend that Ofcom be required to produce an annual report on the impact of regulated services on media plurality.*

Government Response

254. We recognise the importance of being able to ascertain the impact of regulated services on media plurality. In November 2021, Ofcom published their report into the impact on media plurality of issues beyond the scope of the existing regulatory framework, which included issues related to online intermediaries and their algorithms.

255. Ofcom have committed to progressing further work on these issues. Ofcom intends to establish whether and how these issues present concerns for maintaining media plurality in the UK, and to consider what, if any, the potential options for addressing these concerns might be. Ofcom aims to provide its views by the summer of 2022. In light of this, the government does not see the need, at this stage, to put this work on a statutory footing.

Transparency and redress

SUMMARY

- This chapter focuses on transparency – the need for companies to provide information about their activities and the risks on their platforms – and on user redress mechanisms.
- The Joint Committee's recommendations in this area focused on ensuring that the public, independent researchers and Ofcom have access to appropriate data relating to online safety and the actions that platforms are taking to improve safety for their users. The recommendations also seek to ensure that platforms provide suitable internal redress mechanisms for users, and that users have access to external redress mechanisms if they do not receive a satisfactory response from a platform.
- Since publication of the draft Bill, we have developed the Bill further, to:
  - Ensure that services subject to the safety duties make clear to their users in terms and conditions that they have a right of action in civil court to appeal moderation decisions affecting their content.

Joint Committee Recommendation – Current problems underlying transparency reporting (Para 410-411):

256. *We recommend that Ofcom specify that transparency reports produced by service providers should be published in full in a publicly accessible place. Transparency reports should be written clearly and accessibly so that users and prospective users of the service can understand them, including children (where they are allowed to use the service) and disabled people.*

257. *We recommend that the Bill require transparency reporting on a regular, proportionate basis, with the aim of working towards standardised reporting as the regulatory regime matures. The Bill should require minimum standards of accuracy and transparency about how the report was arrived at and the methodology used in research. For providers of the highest risk services, the outcome of the annual audits recommended in paragraph 340 should be required to be included in the transparency report.*

Government Response

258. The government agrees with the Committee that services with transparency reporting requirements should be required to publish their transparency reports in full, and in an accessible and public place. Ofcom will be able to specify in its notice the manner, timescale and the format in which the reports must be published, which will allow them to ensure that reports are easily accessible.

259. The transparency framework will require reporting on a regular basis. Reporting requirements will be annual, and the DCMS Secretary of State will have the power to alter the frequency of the reporting requirements further down the line if necessary. The reporting requirements will be proportionate and reflect the diversity of services in scope. Ofcom will take into account various factors to decide which types of information will be required from these services, including the service provider's capacity, the type of service and the functionalities the service offers, the number of users of the service and the proportion of users who are children.

260. Ofcom will set out the specific information that services need to provide in their reports in the form of notices to the providers. This will ensure that Ofcom can require these services to report on the information which is most useful to Ofcom, to users and to civil society.

261. Ofcom will have the power to specify the metrics companies will need to include in their reports and could require these services to use particular methodologies where necessary. Furthermore, services must ensure that the information provided in a transparency report is complete and accurate or they could face enforcement action. Ofcom will also have the power to require additional information using their comprehensive information gathering powers, including for the purpose of assessing compliance with the transparency reporting requirements.

262. A key objective of transparency reporting is to empower users and allow them to make informed decisions about which services subject to the safety duties they want to use, by comparing the reports. At the same time, it is also important to recognise that there is a diversity of services subject to the safety duties and a one-size fits all approach is unlikely to always be appropriate. Ofcom will have the flexibility to decide on the specific information that services will need to report on and how/to what extent reporting requirements differ between these services. This will help ensure we get the right balance.

Joint Committee Recommendation – Current problems underlying transparency reporting (Para 412):

263. *We agree with the list of information that Ofcom can require as part of its transparency reporting powers and recommend that it should have the clear power to request any other information. We recommend that transparency reporting should aim to create a competitive marketplace in respect of safety, where people can reasonably compare, using robust and comparable information, performance of services as they operate for UK users. We suggest Ofcom also be able to require information be published in transparency reports including (but not limited to):*

a. Safety by design features;

b. Most viewed/engaged with content by month;

c. Most recommended content by month by age group and other demographic information (where that information is collected);

d. Their terms and conditions;

e. Proportion of users who are children;

f. Proportion of anonymous users;

g. Proportion of content breaching terms and conditions;

h. Proportion of content breaching terms and conditions removed;

i. Proportion of appeals against removal upheld;

j. Proportion of appeals against removal, by both recognised news publishers and other users on the grounds of public interest, upheld; and

k. Time taken to deal with reports.

Government Response

264. We agree with the Committee that a key objective of transparency reporting is to empower users by providing them with information about the steps services are taking to keep them safe. This will then drive industry accountability and hopefully encourage a 'race to the top'. Ofcom will have the power to require all services in scope of transparency reporting to report on the information listed by the Committee under the current wording of the Bill. Furthermore, the list of information that Ofcom can require services to include in their transparency reports covers any other steps that a service is taking which relate to online safety matters. This will help future-proof the framework.

Joint Committee Recommendation – Current problems underlying transparency reporting (Para 413):

265. *In addition to transparency reporting, Ofcom should be empowered to conduct its own independent research with the aim of informing the UK public about the comparative performance of services in respect of online safety.*

Government Response

266. The government agrees with the Committee on the benefits of Ofcom conducting its own independent research into online harms, and it is committed to ensuring that Ofcom can access the information it needs to support this.

267. Ofcom will have the power to require information from all services to support its own research activity. Ofcom will be able to publish its research to inform users and civil society about online harms. Ofcom will also be required to produce an annual report on the transparency reports produced by services, which will allow Ofcom to highlight key trends and examples of best practice. This will help users understand what steps services are taking to meet their safety duties and make informed decisions about which services they use.

Joint Committee Recommendation – Access for independent researchers (Para 426 – 430):

268. *The draft Bill requires that Ofcom produce a report on access to data for independent researchers. We recommend work on this report starts as soon as possible. We recommend that Ofcom be given the powers in the Bill to put into practice recommendations from that report.*

269. *Ofcom should have the power i) to audit or appoint a third-party to audit how services commission, surface, collate and use their research; ii) to request a) specific internal research from services; b) research on topics of interest to the Regulator.*

270. Ofcom should commission an independent annual assessment, conducted by skilled persons, of what information should be provided by each of the highest risk services to advance academic research.

271. We recommend that the Bill should require service providers to conduct risk assessments of opening up data on online safety to independent researchers, with some predefined issues to comment on, including:

a. Privacy;

b. Risk of harm to users;

c. Reputational risks (for the service provider) and;

d. Financial cost

272. We recommend that Ofcom should require service providers to conduct an annual formal review of using privacy-protecting technologies and enable them to share sensitive datasets.

Government Response

273. We are supportive of services improving the ability of independent researchers to access their data, subject to appropriate safeguards. This is why 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 services subject to the safety duties to inform their research.

274. After the publication of the report, Ofcom will then have the power to prepare guidance about the issues dealt with by the report for services and people carrying out independent research into online safety. We expect that these provisions will help companies and researchers overcome potential challenges associated with researcher access and will encourage safe and responsible sharing of data for research.

275. Both DCMS and Ofcom understand the Committee's desire for Ofcom to begin work on this report as soon as possible. Between now and Royal Assent, Ofcom will be preparing for its new responsibilities under the Online Safety Bill so that the Bill's provisions can be implemented as quickly as possible. However, its powers and responsibilities under the Bill will only come into effect following Royal Assent. This includes the requirement to prepare a report on researchers' access to information and to consult various stakeholders on that report. It is important to ensure that Ofcom has adequate time to speak to relevant stakeholders and conduct the necessary research and analysis to support this work. The Bill requires Ofcom to publish their report within two years after the Bill comes into force, but they will be able to publish the report sooner.

276. Ofcom will have the power to require information from services subject to the safety duties about how services commission, surface, collate and use their research. Ofcom will also have the power to request services' share specific pieces of internal research, where relevant. Furthermore, the Bill recognises the importance of Ofcom being able to draw on external expertise. Ofcom will also have the power to require services to undergo skilled persons' reports which will allow Ofcom to identify and assess any failure to comply with a relevant requirement under the Bill and also to develop Ofcom's understanding of the risk of a service failing to comply with a relevant requirement, and ways to mitigate such a risk**.**

277. We will consider the additional recommendations on further steps that could be taken in relation to facilitating and/or improving the potential sharing of online safety data with independent researchers.

Joint Committee Recommendation – Redress and reporting mechanisms for in-scope providers (Para 443-444):

278. *The Bill should establish proportionate minimum standards for the highest risk providers' reports, complaints, and redress mechanisms as set out in a mandatory code of practice prepared by Ofcom.*

279. *We recommend a requirement on the face of the Bill for Ofcom to set out: i) how they will assess the a) ease of use; b) accessibility and c) transparency of a service's complaints process for d) adults; e) children; and g) disabled people f) vulnerable adults; ii) what steps Ofcom will be able to take if it finds any of these processes wanting; and iii) how Ofcom will ensure that requirements to operate complaint, reporting and redress mechanisms are proportionate for smaller in-scope providers*

Government Response

280. The government thanks the Committee for raising this issue and recognises the importance of the need for clarity in all the reporting, complaints, and redress mechanisms.

281. The Bill currently places on all services subject to the safety duties a specific legal duty to have effective and accessible user reporting and redress mechanisms. These duties will be bolstered by the material in Ofcom's codes of practice on reporting and redress. The government expects the codes to cover areas such as accessibility (including children), transparency, communication with users, signposting, and appeals.

282. Whilst we agree with the Committee's objectives, to include the requirement set out by the Committee on the face of the Bill would be too prescriptive and could be inflexible. We want Ofcom to be able to respond to changes in the sector, and thus we have not incorporated these requirements into the drafting.

Joint Committee Recommendation – Redress and reporting mechanisms for in-scope providers (Para 445):

283. *Clause 15 (3)(c) should be amended so that it reads "is easy to access, including for disabled people and those with learning difficulties".*

Government Response

284. The government agrees with the Committee that those with a disability, or an adult (such as those with caring responsibilities) providing assistance, must be able to access service providers' user redress provisions. This is an important part of how the Bill will empower those with a disability to keep themselves safe online, and to enjoy their right to freedom of expression. The Equality Act 2010 already includes a duty on service providers to make "reasonable adjustments" to enable disabled persons to access their services. Therefore, although we agree with the Committee about the importance of access for those with a disability, we consider that adding a specific requirement in the Online Safety Bill would be duplicative and would likely cause confusion.

Joint Committee Recommendation – Redress and reporting mechanisms for in-scope providers (Para 446):

285. *Providers of the highest risk services should have to give quarterly statistics to Ofcom on:*

i. Number of user reports;

ii. User reports broken down by the reason the report was made;

iii. Number of actionable user reports;

iv. Actionable user reports broken down by the reason the report was made;

v. How long it took the service provider to respond to
   1. All user reports;
   2. Actionable user reports;

vi. What response was made to actionable user reports;

vii. Number of user complaints received;

viii. Number of actionable user complaints;

ix. How long it took the service provider to respond to
   1. All user complaints;
   2. Actionable user complaints;

x. What response was made to actionable user complaints;

xi. How many pieces of user content were taken down;

xii. How many pieces of content that were taken down were later reinstated;

xiii. The grounds on which content that was reinstated was reinstated;

xiv. How long it took the service provider to reinstate a piece of content that was later reinstated.

Government Response

286. Delivering greater transparency, trust, and accountability is at the heart of the new regulatory framework. In the complex and constantly evolving online world it is crucial that the regulator is well informed, that users are empowered, and that services are held to account for keeping their users safe online

287. Ofcom already has the power to require information from services subject to the safety duties, both in the form of transparency reporting from some services and in response to specific information requests. Ofcom are able to require any relevant information at the frequency required by them to achieve appropriate understanding and assurance of the services' functions. This may be one-off, quarterly, or more frequently dependent on Ofcom's need.

288. For Ofcom to operate effectively they will need to be able to prioritise effectively and request the information from services that is most useful. As such, whilst we support the aim of the Joint Committee's recommendation, we believe a greater degree of flexibility for Ofcom is preferable.

Joint Committee Recommendation – External redress for individuals (Para 457):

289. *The role of the Online Safety Ombudsman should be created to consider complaints about actions by higher risk service providers where either moderation or failure to address risks leads to significant, demonstrable harm (including to freedom of expression) and recourse to other routes of redress have not resulted in a resolution. The right to complain to this Ombudsman should be limited to users to those i) who have exhausted the internal complaints process with the service provider against which they are making their complaint and ii) who have either a) suffered serious or sustained harm on the service or b) had their content repeatedly taken down. There should be an option in the Bill to extend the remit of the Ombudsman to lower risk providers. In addition to handling these complaints the Ombudsman would as part of its role i) identify issues in individual companies and make recommendations to improve their complaint handling and ii) identify systemic industry wide issues and make recommendations on regulatory action needed to remedy them. The Ombudsman should have a duty to gather data and information and report it to Ofcom. It should be an "eligible entity" to make super complaints.*

Government Response

290. The government is committed to ensuring that users of services can complain and seek action both if they encounter harmful content on a service, and if they think that service has treated them or their content unfairly.

291. An independent resolution mechanism such as an Ombudsman is relatively untested in areas of non-financial harm. Therefore, it is difficult to know how an Ombudsman service could function where user complaints are likely to be complex and where financial compensation is not usually appropriate. An Ombudsman service may also disincentivise services from taking responsibility for their users' safety. Introducing an independent resolution mechanism at the same time as the new regime may also pose a disproportionate regulatory burden for services and confuse users.

292. The Secretary of State will be able to reconsider whether independent resolution mechanisms are appropriate at the statutory review. Users will also already have a right of action in court if their content is removed by a service provider in breach of the terms and conditions. We will be requiring services to specifically state this right of action clearly in their terms and conditions.

Joint Committee Recommendation – Liability in civil courts (Para 460):

293. *We believe that this Bill is an opportunity to reset the relationship between service providers and users. While we recognise the resource challenges both for individuals in accessing the courts and the courts themselves, we think the importance of issues in this Bill requires that users have a right of redress in the courts. We recommend the government develop a bespoke route of appeal in the courts to allow users to sue providers for failure to meet their obligations under the Act.*

Government Response

294. The government is committed to understanding users' experiences, detecting issues early and addressing their concerns diligently through thorough processes.

295. Individuals are currently able to 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. We will be clarifying the right of users of user-to-user services subject to the safety duties to bring claims for breach of contract for wrongful

removal or restriction of content by requiring these services to inform users of that right in their terms and conditions. Over time, as regulatory precedent grows, it will become easier for individuals to take user-to-user services to court when necessary.

296. Introducing a tribunal for online harms complaints could disincentivise user-to-user services subject to the safety duties to take more responsibility for their users' safety. It could also place a disproportionate financial burden on these services and/or the justice system.

Joint Committee Recommendation – Access to data in cases of bereavement (Para 463):

297. *Bereaved parents who are looking for answers to the tragic deaths of their children in their digital data should not have to struggle through multiple, lengthy, bureaucratic processes to access that data. We recognise that an automatic right to a child's data would raise privacy and child safety concerns. At the same time, we believe there is more than could be done to make the process more proportionate, straightforward and humane. We recommend that the government undertake a consultation on how the law, and service's terms and conditions, can be reformed to give access to data to parents when it is safe, lawful and appropriate to do so. The government should also investigate whether the regulator could play a role in facilitating co-operation between the major online service providers to establish a single consistent process or point of application.*

Government Response

298. The government recognises the difficulties some bereaved parents have experienced when accessing their loved ones' data. We understand that some companies operate policies of non-disclosure to third parties (including parents), unless a user takes active steps to nominate a person who may access his or her account after they die or where there is a legal obligation to disclose the data. As the Committee notes, an automatic right of access is unlikely to be appropriate in every case and some people might be concerned about the disclosure of private information or other digital assets to third parties after their death. As it stands, disclosure of data relating to a deceased person falls outside the scope of this Bill, and is not prevented by the UK's data protection legislation.

299. The Committee rightly notes that legislation may not be the only or an effective solution. Raising public awareness about how to make provisions for access to personal data after death may also form part of the answer. The government will consider these matters further before deciding on next steps.

Joint Committee Recommendation – Access to data in cases of bereavement (Para 464):

300. *We also recommend Ofcom, the Information Commissioner and the Chief Coroner review the powers of coroners to ensure that they can access digital data following the death of a child. We recommend the government legislate, if it is required, to ensure that coroners are not obstructed by service providers when they require access to digital data. We recommend that guidance is issued to coroners and regulatory authorities to ensure they are aware of their powers in dealing with service providers and of the types of cases where digital data is likely to be relevant. Our expectation is that the government will look to implement the outcomes of these consultations in the Bill during its parliamentary passage.*

Government Response

301. We note the concerns raised by the Joint Committee in this area, but note that coroners already have statutory powers to require evidence to be given or documents to be produced for the purpose of their inquests (which would include relevant digital data following the death of a child) with sanctions where such evidence is not given, or documents produced, and they are well aware of these powers.

Annex A – Priority Offences in the Online Safety Bill

Below is a list of offences we propose to include in the Online Safety Bill.

- Encouraging or assisting suicide
- Offences relating to sexual images, including revenge and extreme pornography
- Incitement to and threats of violence
- Hate crime
- Public order offences, harassment and stalking
- Drug-related offences
- Weapons and firearms offences
- Fraud and financial crime
- Money laundering
- Exploiting prostitutes for gain
- Organised immigration offences

Offences relating to terrorism and child sexual abuse and exploitation are already listed in the Bill. The Secretary of State will have the ability to designate additional offences as priority by statutory instrument, which will be subject to parliamentary scrutiny.

HM Government

E02721600
978-1-5286-3231-7