House of Commons

Digital, Culture, Media and Sport Committee

The Draft Online Safety Bill and the legal but harmful debate

Eighth Report of Session 2021–22

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 20 January 2022

HC 1039
Published on 24 January 2022
by authority of the House of Commons

The Digital, Culture, Media and Sport Committee

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

Current membership

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

Kevin Brennan MP (*Labour, Cardiff West*)

Steve Brine MP (*Conservative, Winchester*)

Alex Davies-Jones MP (*Labour, Pontypridd*)

Clive Efford MP (*Labour, Eltham*)

Julie Elliott MP (*Labour, Sunderland Central*)

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

Simon Jupp MP (*Conservative, East Devon*)

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

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

Giles Watling MP (*Conservative, Clacton*)

Powers

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

Publication

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

Committee staff

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

Contacts

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

You can follow the Committee on Twitter using @CommonsDCMS.

Contents

Summary

The UK Government's Draft Online Safety Bill is an ambitious, complex and contested piece of legislation. Through a series of interlocking duties and suite of enforcement and redress powers and mechanisms, it aims to make user-to-user and search service providers more accountable for the decisions they make when designing the platforms and the systems and processes that govern them. We welcome the Government's decision, as per our previous recommendation, to publish the Draft Bill in full and engage proactively with the various committees, including our own, who have conducted comprehensive pre-legislative scrutiny.

However, there are several areas where existing pre-legislative scrutiny has missed an opportunity and must go further. We have urgent concerns that, as currently drafted, the Bill neither adequately protects freedom of expression nor is clear and robust enough to tackle the various types of illegal and harmful content on user-to-user and search services. We have proposed several amendments to the definition and scope of harms covered by the regime that would bring the Bill into line with the UK's obligations to freedom of expression under international human rights law. We also recommend that the Government proactively address types of content that are technically legal, such as insidious parts of child abuse sequences like breadcrumbing and types of online violence against and women and girls like tech-enabled 'nudifying' of women and deepfake pornography, by bringing them into scope either through primary legislation or as types of harmful content covered by the duties of care.

Moreover, we have found that current provisions that provide Ofcom with a suite of powers and users with redress are similarly unclear and impractical. We urge the Government to provide greater clarity within the Bill on how and when these powers should be used to ensure they are both practical and proportionate. Finally, we are concerned that the Joint Committee's recommendation to replace independent, elected, cross-party select committees with a joint committee created by Government would undermine, rather than enhance, parliamentary scrutiny.

1 Pre-legislative scrutiny

1. The UK Government's long-awaited Draft Online Safety Bill is an ambitious, complex and, above all, contested piece of legislation. The origins of the Bill date back to the Internet Safety Strategy Green Paper, though the regime proposed by the Bill has undergone significant changes. Since the beginning of this Parliament, we have pushed for the Bill to be published in draft form and stated our intent to conduct pre-legislative scrutiny.[1] The Bill has animated interlocutors across Parliament, academia, civil society, industry and the general public and, if likeminded legislation across the world is any measure, will likely continue to do so long after it receives Royal Assent. In particular, we have heard about critical issues that need to be focussed on before the Bill is introduced and scheduled for its Second Reading. These include: concerns regarding freedom of expression, whether the Bill adequately addresses child sexual exploitation and abuse (CSEA), key omissions such as violence against women and girls (VAWG) and harms to democracy, and the need for a proportionate yet clear and robust enforcement framework. For its part, the Government has said that it will consider the recommendations we bring forward.[2]

2. This Report addresses issues that we consider need to be the subject of public debate as soon as possible regarding the Draft Online Safety Bill. This Report does not represent the end of our interest in the Bill and related matters. We will continue to undertake evidence sessions, as well as draw on the testimonies we have received to date, and will produce further Reports on the online safety regime and other areas of digital regulation as the Online Safety Bill progresses through the House. In this Report we make several conclusions in key and urgent areas that many stakeholders, in evidence to our Sub-Committee, feel are yet to be addressed by the Draft Bill and pre-legislative scrutiny. We are grateful to the many stakeholders who have contributed extensive oral and written evidence over the last few months in particular (more than has directly featured in this Report) but has nonetheless informed our position in all areas of this legislation.

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

1 Digital, Culture, Media and Sport Committee, Second Report of the Session 2019–21, Misinformation in the COVID-19 Infodemic, HC 234, para 12

2 Oral evidence taken before the Liaison Committee on 17 November 2021, HC 835, Q 55; HC Deb, 13 January 2022, cols 754–5 [Commons Chamber]

2 The duty of care

The proposed duty of care model

Proposed definitions and types of harm

4. Though the framework introduced by the Draft Online Safety Bill is referred to in discourse as 'the Duty of Care', the Draft Bill itself does not establish an overarching or general duty on service providers. Instead, it provides several specific duties[3] that together require providers to take steps to mitigate and manage the risks of harm from three broad typologies of content:

- illegal content;
- content that is harmful to children; and,
- for 'high-risk, high-reach' user-to-user services[4], content that is harmful to adults.[5]

Illegal content[6] is defined in the Bill as "content consisting of certain words, images, speech or sounds" where the use (inherently or when taken together with other regulated content) or dissemination amounts to or constitutes a relevant offence.[7] Relevant offences are terrorist and CSEA content, offences specified in regulations made by the Secretary of State ('priority illegal content'), or offences in which the victim or intended victim is an individual or individuals.[8] However, three types of wrongs are also specifically precluded from the illegal content typology: namely the infringement of intellectual property rights, the safety and quality of goods and the performance of a service by someone not qualified to perform it.[9]

5. Content that is harmful to children and content that is harmful to adults, meanwhile, are defined in similar ways to one another:

3 Part 2, Chapter 2 provides duties of care for providers of user-to-user services; Part 2, Chapter 3 provides duties of care for providers of search services. The duties of care detailed in these parts are delineated by the Bill thusly: risk assessment duties; safety duties; duties about freedom of expression, privacy and so on; user reporting and redress duties; and record-keeping and review duties. The duties on providers of user-to-user services are more extensive than those on providers of search services. Definitions are provided in Part 2, Chapter 6.

4 The Draft Bill divides services into three categories: Category 1 (which the Government envisages would be these high-risk, high-reach user-to-user services); Category 2A (all regulated search services); and Category 2B services (the remainder of regulated user-to-user services). The Bill provides Category 1 services with additional duties, such as safety duties for content that is harmful for adults, duties to protect journalistic content and content of democratic importance, and duties to carry out assessments on the impact of safety policies and procedures on impacts to freedom of expression and privacy. Schedule 4 requires the Secretary of State to make regulations specifying the precise threshold conditions for Category 1 services with respect to the number of users and functionalities. The Joint Committee on the Draft Online Safety Bill has recommended that the Government remove these categories entirely.

5 Draft Online Safety Bill, CP 405, May 2021, clauses 41, 45, 46

6 Established in the safety duties in Clause 9 for user-to-user services and Clause 21 for search services and defined in Clause 41.

7 Draft Online Safety Bill, CP 405, May 2021, clause 41(3)

8 Draft Online Safety Bill, CP 405, May 2021, clause 41

9 Draft Online Safety Bill, CP 405, May 2021, clause 41(6)

- either as content of a type that is designated in regulations made by the Secretary of State,[10] or
- as "non-designated content" that fulfils one of the general definitions.[11]

These general definitions apply to content that is not specifically mentioned in on the face of the Bill or made through regulations but where the provider of the service has reasonable grounds to believe that the nature or dissemination[12] of the content is such that there is a material risk of it having, or indirectly having, a significant adverse physical or psychological impact on a child or adult (as applicable in the relevant clause) of ordinary sensibilities.[13]

6. The definitions underpin risk assessment duties for both content typologies. In particular, the general definitions provide the basis for identifying types of prominent non-designated content. These definitions also underpin the relevant safety duties:

- For content that is harmful to children, this includes: duties to take proportionate steps and operate proportionate systems and processes to prevent and protect children from encountering harmful content; maintaining detailed, clear and accessible terms of service; and ensuring that these terms of service are applied consistently.[14] The safety duties regarding content that is harmful to children apply to all user-to-user and search services.
- For content that is harmful to adults, this only includes duties to maintain detailed, clear, accessible and consistently-applied terms of service.[15] As noted above, the safety duties for content that is harmful to adults only applies to Category 1 services, which the Government has argued will comprise high-risk, high reach user-to-user services and be designated through regulations.

In both instances, the risk assessment duties theoretically flow through to the relevant safety duties, which codifies how risks of harm are first identified and then mitigated and managed.[16] While this approach, in its totality, is complex, there are many areas that remain vague or undefined and as such may not provide a comprehensive safety regime.

Balancing freedom of expression

7. Though the proposed duty of care model is therefore undoubtedly complex, it has been broadly welcomed by many. Academics have welcomed the duty of care as superior to the "intermediary liability" model used in jurisdictions such as Germany because it makes providers liable for their own conduct (defined as a lack of diligence to adopt preventative or remedial measures, systems and processes) rather than the conduct of

10 These designations are, for content that is harmful to children, either "primary priority content that is harmful to children" or "priority content that is harmful to children", and, for content that is harmful to adults, "priority content that is harmful to adults". This is set out in clauses 45(2) and 46(2).

11 Draft Online Safety Bill, CP 405, May 2021, clauses 45(3), 45(5), 46(3), 46(5)

12 In the case where the material risk comes from the fact of the content's dissemination, explicit reference is made to how many users may be assumed to encounter the content when using the service and how easily, quickly and widely the content may be disseminated through it.

13 Draft Online Safety Bill, CP 405, May 2021, clauses 45, 46

14 Draft Online Safety Bill, CP 405, May 2021, clause 10

15 Draft Online Safety Bill, CP 405, May 2021, clause 11

16 Draft Online Safety Bill, CP 405, May 2021, clauses 10(7), 11(4)

others (expressed as the content and activity on their services).[17] Ofcom similarly has noted that the principles-based focus on the design of systems and processes will allow regulation to respond at speed and place the burden of identifying and addressing risks of harm on the industry itself, which it considers is best placed to design technical solutions and be held to account for their success or failure.[18] However, debates around the regime have predominantly made reference to whether they proportionately balance human rights, and particularly the rights to freedom of expression and respect for privacy.

8. Currently, the Draft Bill provides duties on providers (and Ofcom) to have regard to the importance of the right to freedom and expression and privacy in various ways.[19] However, as Lexie Kirkconnell-Kawana, Head of Regulation at IMPRESS, told us, "freedom of expression protections in the Bill […] are very weak" and "the due consideration and due regard statements of intent in this Bill are very ineffectual".[20] She further argued that "I think you will see very low compliance with that requirement".[21] As such, it is equally important that these rights are reflected not only in the requirements to consider freedom of expression but also in the drafting of the safety and risk assessment duties themselves.

9. As we discussed in our Report on *Misinformation in the Covid-19 Infodemic* (published before the Draft Bill was brought forward by the Government) and has been reiterated by legal experts throughout the pre-legislative scrutiny process, any prohibition or limitation to freedom of expression, whether by criminal, civil or administrative means, must be necessary and proportionate to achieve a legitimate aim and have a clear and precise legal basis under the UK's obligations regarding international human rights law.[22] These principles are well established in treaties such as the International Covenant on Civil and Political Rights (ICCPR) and European Convention on Human Rights (ECHR) and codified in UK law by the Human Rights Act 1998.[23] Moreover, as Dr Talita Dias notes, these specific international instruments require the UK to follow a tiered or structured approach to the regulation of any content depending on the legal category under which it falls, such as whether certain types of speech are prohibited[24], limited[25] or protected or free speech.[26] Indeed, reflecting these obligations, we recommended in our previous Report that "legislation should also establish clearly the differentiated expectations of tech companies for illegal content and 'legal but harmful'".[27] Discussing moderation practices of in-scope services both currently and proposed under the online safety regime, the

17 Qq 1–4, 7; Dr Talita Dias (OSH0090)
18 Ofcom (OSB0021)
19 Draft Online Safety Bill, CP 405, May 2021, clauses 12, 13, 14, 23, 29(5), 31(6), 50(2), 106
20 Q 166
21 Q 166
22 Digital, Culture, Media and Sport Committee, Second Report of the Session 2019–21, Misinformation in the COVID-19 Infodemic, HC 234, paras 13–17; Dr Talita Dias (OSH0006); Dr Talita Dias (OSH0090); see also Oral evidence taken before the Joint Committee on the Draft Online Safety Bill on 23 September 2021, HC 609, Q 69 [Dr Edina Harbinja]; Oral evidence taken before the Joint Committee on the Draft Online Safety Bill on 21 October 2021, HC 609, Q 135 [Barbora Bukovská]
23 Dr Talita Dias (OSH0006); Big Brother Watch (OSH0054); see also United Nations Human Rights, International Covenant on Civil and Political Rights, accessed 10 January 2022; Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, accessed 10 January 2022
24 Such as that detailed in Article 20 of the ICCPR. For example, advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.
25 Such as in Article 19(3) ICCPR. For example, limitations in order to respect the reputations of others or to protect national security, public order, public health or morals.
26 Dr Talita Dias (OSH0006); Dr Talita Dias (OSH0090)
27 Digital, Culture, Media and Sport Committee, Second Report of the Session 2019–21, Misinformation in the COVID-19 Infodemic, HC 234, para 16

Turing Institute wrote that, with respect to in-scope services, "outside of illegal content and activity, platforms set policies based on their social values and the proposition that they offer to users", which must balance protecting users from harm and protecting users' freedom of expression, and that this "spectrum of hazard tolerance should be reflected in the [Online Safety Bill]".[28] Whilst the Government has attempted to do this (such as by delineating duties to identify, manage and mitigate the risk of harms with respect to the three content typologies and by further categorising services based on risk and reach), it is clear that several weaknesses remain.

Definitions of harm

Illegal content

10. A primary weakness of the Draft Bill concerns the overarching definitions of harm. There has been consensus across stakeholders that tackling illegal content online should be a priority for the online safety regime.[29] Despite this, the Bill itself is vague about the precise scope of illegal content, seemingly conflating criminal offences with civil and administrative wrongs. Dr Dias argued that "we don't know exactly which among these, criminal or not criminal, illegal acts going to fall within the scope of the Bill" and thus entail the most stringent measures.[30] Similarly, evidence from the British Board of Film Classification argued that whilst the regime currently "specifically includes CSEA and terrorism content and activity as priority illegal content", it is "less clear on other types of illegal content that platforms will be required to act against".[31] These sentiments have been echoed by the private sector, including techUK (the trade body that includes in-scope services), BT, TSB Bank, UK Finance, the Association of British Insurers and the Pensions and Lifetime Savings Association.[32] Whilst a charitable reading of the Bill would imply that the Government seemingly attempts to do this by excluding three specific civil wrongs, the Bill is unclear overall about the extent of illegal content it aims to tackle. ***The Government should redraft the Online Safety Bill to state explicitly that the scope of the framework for addressing "illegal content", which should be subject to the most stringent moderation measures, specifically applies to existing criminal offences, rather than regulatory offences and civil or administrative wrongs.***

28 Alan Turing Institute, Public Policy Programme (OSH0007)

29 Glitch (OSH0013); Centenary Action Group, Glitch, Antisemitism Policy Trust, Inclusion London, Stonewall, Compassion in Politics, Women's Equality Party, The Traveller Movement, Women's Aid Federation of England (Women's Aid), Girlguiding, The Jo Cox Foundation, Imkaan and End Violence Against Women Coalition (OSH0014); CEASE UK (OSH0015); Coalition for a Digital Economy (Coadec) (OSH0021); Reset (OSH0024); Trustpilot (OSH0037); Open Rights Group (OSH0039); Refuge (OSH0041); Legal to Say, Legal to Type (OSH0042); Big Brother Watch (OSH0054); techuk (OSH0075); NSPCC (OSH0076); Nuffield Council on Bioethics (OSH0077); Internet Service Providers' Association (ISPA) (OSH0083); #NotYourPorn, Chayn, Dr Fiona Vera Gray, End Violence Against Women Coalition (EVAW), Faith & VAWG Coalition, Glitch, Imkaan, Professor Clare McGlynn, Rape Crisis England & Wales, Refuge, Welsh Women's Aid, Women & Girls Network (WGN), Women's Aid Federation England (OSH0083); Quilter (OSB0024); Full Fact (OSB0056); British Horseracing Authority (OSB0061)

30 Qq 1, 18

31 BBFC (OSB0006)

32 Association of British Insurers (OSH0044); PLSA (OSH0046); UK Finance (OSH0051); TSB Bank (OSH0063); BT Group (OSH0074); techUK (OSH0075)

Provisions to protect children

11. The Government has emphasised since the Online Harms White Paper that the regulatory regime should provide particular protections for children online.[33] Child sexual exploitation and abuse (CSEA) still constitutes a significant issue: last year alone, the Internet Watch Foundation removed 153,000 webpages of child sexual abuse constituting millions of images, but has seen exponential growth in the rise in self-generated content.[34] Evidence also shows a gendered element to CSEA, with 80 percent of sexual communication with a child offences being perpetrated against girls.[35] The National Crime Agency currently estimates that there are between 500,000 and 850,000 people with a sexual interest in children in the UK.[36] Meta Platforms-owned apps account for more than half of grooming offences, with Instagram posing an increasing problem year-on-year in terms of total offences but also as a proportion of offences.[37] Ultimately, witnesses concluded that the failings of Meta in particular to address child safety had arisen because these concerns were considered secondary to profit.[38] There are several ways the Draft Bill proposes to remedy this, such as by prioritising CSEA amongst other types of illegal content, by providing more granular ways of designating content within the typology of content that is harmful to children (as well as the general definition for non-designated content),[39] and duties on providers to assess whether their services can be accessed by children.[40] The Joint Committee on the Draft Online Safety Bill[41] has made several further interventions[42] that we support and would expect the Government to accept, namely:

- that age-inappropriate or otherwise inherently harmful content and activity (like pornography, violent material, gambling and content that promotes or is instructive in eating disorders, self-harm and suicide)[43] should appear on the face of the Bill;
- that the Bill incorporate duties to co-operate in tackling cross-platform harms;[44]
- for the regime to set out minimum standards for privacy-protecting, rights-enhancing age assurance (with reference to the recent ICO opinion on the Age-Appropriate Design Code);[45]

33 Department for Digital, Culture, Media and Sport and Home Office, Online Harms White Paper, CP 57, 8 April 2019
34 Qq 34, 48, 89–94
35 Q 70
36 Qq 34, 106–8
37 Qq 51–2
38 Qq 55, 94–9
39 These are duties for primary priority content that is harmful to children, which requires providers to use proportionate systems and processes to prevent children of any age encountering that content, and duties for priority content that is harmful to children, which requires providers to use proportionate systems and processes to prevent children from age groups judged to be at risk of harm from encountering it.
40 Draft Online Safety Bill, CP 405, May 2021, clauses 9, 10, 21, 21, 26
41 Hereafter referred to as 'the Joint Committee'.
42 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, paras 202–4, 235–7
43 Q 77
44 Qq 40–43, 74–6
45 Qq 46–7, 79

- and for the Government to close the 'OnlyFans loophole' for the "likely to be accessed by children" test, explained to us by Andy Burrows, where a site like OnlyFans could legitimately argue that it should not be in scope because children did not constitute a significant portion of its user base.[46]

12. Despite this, the Bill does have weaknesses where the regime does not map adequately onto the reality of the problem. We heard that particular social networking sites are a key vector in the creation of new child abuse images as well as cross-platform grooming.[47] Furthermore, the Bill contains weaknesses regarding content and activity that is specifically designed to evade or subvert content moderation. One such type of activity is "breadcrumbing", which refers to public content and activity, designed or calculated with a clear sense of subverting online content moderation rules, but does not meet the criminal threshold for removal. Andy Burrows, Head of Child Safety Online Policy at the NSPCC, described the problem posed by breadcrumbing for children's safety:

> They know what they can post and what they cannot. This could be tribute sites, pictures of a child that to you and me would be perfectly innocuous but if you are an abuser you will recognise the context behind it. These are carefully edited child abuse sequences, so they are edited in such a way that they are on the right side of what platforms will keep up rather than take down. They effectively allow child abusers to use platforms as an online shop window to advertise their sexual interest in children and then in turn to form networks that will go off platform to encrypted sites, to less scrupulous platforms where abuse material can be shared. As it stands in this Bill we are concerned about whether that content will be actioned and that is a product of the Bill having the separate buckets between illegal and legal activity. There is a risk that this falls into a grey area where it is not captured because it is not illegal content.[48]

Though the Bill takes several welcome steps to address harms to children, such as duties to tackle child sexual exploitation and abuse (CSEA), we are concerned about the prevalence of content and activity that are seemingly not captured by the proposed regime. One example of such activity is breadcrumbing, where perpetrators deliberately subvert the thresholds of criminal activity and for content removal by a service provider. *We recommend that the Government respond to our concerns about the risk of content and activity that falls below the threshold of outright criminal activity but nonetheless forms part of the sequence for online CSEA. One starting point should be to reframe the definition of illegal content to explicitly add the need to consider context as a factor, and include explicitly definitions of activity like breadcrumbing, on the face of the Bill.*

Content that is harmful to adults

13. Of particular contention are the duties regarding content that is harmful to adults, both for people who generally support and oppose the provisions set out in the Bill. Tech companies and privacy campaigners have called for the removal of these provisions altogether. For instance, techUK argues that the duties, as currently drafted, could create

46 Qq 77–8
47 Qq 39–43
48 Q 56

requirements to "prevent access to a wide range of lawful content".[49] Coadec, Open Rights Group, Big Brother Watch and Legal to Say, Legal to Type similarly warned that overregulation of content would lead to censorship, as well as inviting legal challenge and favouring large incumbents in the market.[50]

14. However, Reset, a civil society organisation, commended the Government for including legal but harmful content in the Bill, citing the need to tackle "abuse and hate witnessed by many on a daily basis such as Covid disinformation, bullying, climate change denial, pro-suicide and self-harm material, none of which is illegal and all of which can have a devastating impact".[51] The submission did note the challenges to freedom of expression, and instead argued for more emphasis on systems and processes to increase friction on the spread of legal but harmful content such as "by focusing on preventative measures such as reduced amplification, demonetisation and targeting".[52] Moreover, many charities committed to ending violence against women and girls (VAWG) warned that the current provisions would not adequately address the extent of harms facing women and girls.[53] As Seyi Akiwowo, founder and Executive Director of Glitch, a charity committed to ending violence against women, noted in oral and written evidence:

> when talking about gender-based online abuse, the vast majority of online abuse against women falls into the "legal but harmful" category[54]

and that:

> the removal of the "legal but harmful" regulations in the Bill would weaken the legislation with regards to ending online violence against women.[55]

Indeed, Ms Akiwowo told us that "women are 27 times more likely to be harassed" and that "it is worse for women of colour, worse for women with disabilities, worse for women from LGBTQI+ communities".[56] Similarly, Marianna Spring, BBC specialist disinformation reporter, and Michelle Stanistreet, General Secretary of the National Union of Journalists, have also highlighted that women in the public eye, such as journalists and politicians, and in public service, like doctors and nurses, receive significant amounts of abuse, which is exacerbated when their position intersects with other identities, such as race and sexual orientation.[57] Ms Stanistreet also emphasised that online harms often continued offline, stating that "it is not that it is more acceptable if it is confined simply to threats coming through your social media, to your email or on your computer screen, but we see cases where that migrates to in-person harassment, abuse and stalking".[58] Despite this, victims

49 techuk (OSH0075)
50 Coalition for a Digital Economy (Coadec) (OSH0021); Open Rights Group (OSH0039); Big Brother Watch (OSH0054); Legal to Say, Legal to Type (OSH0042)
51 Reset (OSH0024)
52 Reset (OSH0024)
53 Glitch (OSH0013); Centenary Action Group, Glitch, Antisemitism Policy Trust, Inclusion London, Stonewall, Compassion in Politics, Women's Equality Party, The Traveller Movement, Women's Aid Federation of England (Women's Aid), Girlguiding, The Jo Cox Foundation, Imkaan and End Violence Against Women Coalition (OSH0014); Refuge (OSH0041)
54 Glitch (OSH0013)
55 Glitch (OSH0013)
56 Q 122
57 Qq 135, 145–6, 186–92
58 Q 187

have little access to recourse from service providers; a recent NUJ member survey, for example, revealed that only 34 percent of respondents reported abuse to social media platforms, while 80 percent said that reporting abuse made no difference whatsoever.[59]

15. Moreover, Rt. Hon Maria Miller MP, Refuge's Senior Policy and Public Affairs Manager Cordelia Tucker O'Sullivan, Ms Akiwowo and Ms Spring all warned against the reductionism of constructing a false dichotomy between addressing harms such as online VAWG and protecting the right to freedom of expression, given that the nature of harms like online abuse can and does chill the freedom of expression of marginalised groups.[60] Evidence from Glitch noted, for example, that despite 96 percent of participants in their workshops found these workshops valuable, due to developing the skills to feel safer and more resilient online, over 69 percent said that they would continue to self-censor due to anxiety and fear of how others would respond.[61]

16. It should be noted that our Report, *Misinformation in the Covid-19 Infodemic*, expressed concern "about deferring responsibility for the scope of restrictions to speech to tech companies" and that current "discussions between tech companies and public authorities [to tackle harms like misinformation] lack transparency, scrutiny and an underlying legal framework", subsequently asserting that this process should be democratic.[62] Though the Joint Committee concluded that the safety duties for content that is harmful to adults were likely intended "primarily as a transparency measure over something companies are already doing", it ultimately recommended that the duties be removed entirely and replaced with a list of types of harm. Stakeholders on both sides of the debate have expressed publicly and privately, however, that the Joint Committee's replacement duty (discussed further in paragraph 27) simply rebrands the current duties and does not address the fundamental issues.[63]

17. As such, there are clearly issues that must be addressed if the regime is to strike an appropriate balance between freedom of expression and tackling these typologies of content. Dr Dias has argued that the definitions of harm provided by the Bill are too vague, with a low evidentiary threshold, and are subjective without providing additional criteria to consider when making a judgement to risk of harm.[64] This is compounded by the fact that the Bill emphasises remedial measures over preventative measures focusing on content dissemination and amplification, and moreover does not illustrate preventative moderation measures other than content takedowns.[65] Notably, the Democracy and Digital Technologies Committee, chaired by Lord Puttnam, similarly concluded that banning or removing legal content outright would limit freedom of expression.[66] Additionally, the definition's emphasis on psychological and physical harm to the individual seemingly deliberately precludes "generic" or "societal" harms (beyond in "special circumstances"

59 The National Union of Journalists (NUJ) (OSH0026); see also Q 189
60 Q 121
61 Glitch (OSH0013)
62 Digital, Culture, Media and Sport Committee, Second Report of the Session 2019–21, Misinformation in the COVID-19 Infodemic, HC 234, para 14
63 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, paras 174–180
64 Qq 2, 3, 11
65 Qq 4, 11, 18, 25, 30; Dr Talita Dias (OSH0006); Professor Alan Renwick and Alex Walker (OSH0040); Dr Talita Dias (OSH0090)
66 Professor Alan Renwick and Alex Walker (OSH0040)

to address threats to national security or the health and safety of the public) that Professor Alan Renwick referred to, in evidence, as harms to democracy such as mis- and disinformation.[67]

18. This has two obvious impacts. First, the Bill does not provide a clear legislative basis upon which Ofcom will be able to judge the efficacy of measures, systems and processes (particularly algorithms and automated systems) in mitigating or managing the risk of such content. Second, the Bill lacks proportionality in this area and may result in excessive takedowns by service providers, especially where their terms and conditions specify that such content should be removed *prima facie* in order to meet the duties' requirements to enforce their terms of service consistently and thus avoid associated penalties.[68] As IMPRESS's Lexie Kirkconnell-Kawana noted:

> The Bill could set out some terms of reference that could neatly align with the system design. Platforms would support that. Platforms are looking for scalable solutions.[69]

There are many measures that could instead be deployed: Lord Puttnam, for instance, told us that it would be more practical to address dissemination of harmful content through automated systems, whilst Professor Renwick recommended measures like flagging, fact-checking and promoting media literacy and accurate, accessible information.[70] Demos similarly lists "reporting processes and resources offered, behavioural nudges, user powers to shape their online experience, support and incentivisation for communities setting their own standards, content interaction and labelling systems, content curation systems and promotion systems, and data collection and tracking systems" as illustrative measures.[71]

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

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

67 Qq 21–2; see also Draft Online Safety Bill, CP 405, May 2021, clauses 29(6), 112
68 Q 11
69 Q 171
70 Qq 4, 9–12
71 Demos (OSH0033)

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

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

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

Designation of types of harm

24. The vagueness, breadth and need for greater granularity of the definitions of harm and the regime more broadly can also be addressed by specifying types of harm that fall into the typologies on the face of the Bill. As our Report, *Misinformation in the Covid-19 Infodemic*, made clear:

> *We strongly recommend that the Government bring forward a detailed process for deciding which harms are in scope for legislation. This process must always be evidence-led and subject to democratic oversight, rather than delegated entirely to the regulator.*
>
> […] *The Government should set out a comprehensive list of harms in scope for online harms legislation, rather than allowing companies to do so themselves or set what they deem acceptable through their terms and conditions.*[72]

However, as the NSPCC's Andy Burrows noted, "so much of the Bill is effectively a scaffold for the secondary legislation, the codes and the guidance that will flow through, there is so much that we cannot pin down at this stage".[73] The failure to include either an illustrative or more comprehensive accompanying list of types of harm has instead opened the regime to several legitimate criticisms.

25. Many groups have expressed concern that certain types of illegal activity will not be adequately addressed or fall under an exemption outlined in provisions on illegal content. This has led to campaigns to include types of economic crime (such as fraud and scams, which the Joint Committee has endorsed including) and violence against women and girls

72 Digital, Culture, Media and Sport Committee, Second Report of the Session 2019–21, Misinformation in the COVID-19 Infodemic, HC 234, paras 16, 72

73 Q 68

that already constitutes criminal behaviour on the face of the Bill.[74] Whilst officials from the Department for Digital, Culture, Media and Sport have tried to reassure parliamentarians and stakeholders on this, clearly tensions remain that could be practically and proactively addressed.[75] Subsequently, this may invite a considerable number of further amendments to the Bill as it passes through Parliament. Written evidence to us suggested several of the most relevant criminal offences that could and should be included in a new Schedule, such as:

- Parts III and Part 3A of the Public Order Act 1986;
- Sections 1–3A of the Computer Misuse Act 1990;
- Sections 125–127 of the Communications Act 2003;
- the Sexual Offences Act 2003;
- Sections 1–11 of Fraud Act 2006;
- the Criminal Justice and Immigration Act 2008; and
- the Criminal Justice and Courts Act 2015.[76]

Whilst the Bill provides procedure for making regulations regarding the categories of regulated services, it does not similarly include procedures for adding types of harm to the Bill.[77] ***The Government should add a new Schedule to the Bill providing at least the most relevant types of illegal content and non-exhaustive illustrative lists of proportionate preventative and remedial measures to mitigate and manage risk. It should also provide, in another new Schedule, a detailed procedure for designating new and/or additional offences that constitute illegal content in the Bill through regulations. Alongside the Bill, the Government should issue example Regulations to illustrate how this process would work and ensure it is done consistently post-implementation.***

26. The Bill is similarly vague on how types of content that is harmful to children and adults might be set out in the Bill. Andy Burrows, for example, told us that I don't think any of us, including Ofcom, know what […] the shape of the regime will look like" and urged the Government to clarify its position on the Law Commission's recommendations.[78] Susie Hargreaves, CEO of the Internet Watch Foundation, noted that:

> The priority content needs clarification, particularly for the "lawful but awful" images. The IWF often find that we have a series of images where we cannot take action on a number of them because they do not meet the legal threshold. The projects when we are working with NSPCC where a young person can self-refer an image of themselves at the moment might not meet

74 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, paras 186–195; et al x 2 and refuge, glitch

75 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 23 November 2021, HC 44, Q 253 [Sarah Connolly]

76 Dr Talita Dias (OSH0090); BBFC (OSB0006)

77 Draft Online Safety Bill, CP 405, May 2021, Schedule 4

78 Qq 67–8 [Andy Burrows]

> our legal threshold but might be causing them real distress, so it is having the ability to remove that. There is a number of cases where the priority content on the margins of what is illegal need to clarified.[79]

These concerns were shared by the tech sector who, through their trade association techUK, stated that "legislation must outline all of the types of harmful content which will be in scope with codes of practice providing descriptions of the types of content which should be interpreted as harmful or not harmful towards adults or children".[80] techUK also echoed the recommendations of our previous Report about how types of harm should be added, arguing that "an evidence-led and democratic process is needed to identify future harms, as well as to evaluate the levels of risk associated with existing harms and whether they should remain in scope".[81]

27. As noted, the Joint Committee has recommended replacing the provisions for content that is harmful to adults. However, it proposes replacing these provisions with a provision to create a list of "reasonably foreseeable risks of harm arising from regulated activities defined under the Bill".[82] This has raised several concerns. First, the Joint Committee's illustrative list seemingly conflates illegal speech (such as hate speech offences, including communication which is threatening or abusive and is intended to alarm, distress or harass), content that will amount to an offence if the Government implements recent recommendations from the Law Commission, and legal but harmful content (such as disinformation and content intended to promote eating disorders and self-harm).[83] Second, the replacement provision retains many aspects of the existing provisions, including a mechanism to add to this list over time.[84] Finally, the Joint Committee's list overlooks the fact that the list provided may not fully address violence against women and girls (VAWG) and other marginalised groups beyond hate speech. Rt. Hon Maria Miller MP detailed specific types of VAWG that are currently legal, including cyber-flashing, intimate image abuse, and using deepfakes and the "nudifying" of women[85] by technological means.[86] Other means by which types of online VAWG might be brought onto the statute books have been criticised as potentially ineffective, meaning that these issues may continue to persist even if the Government tried to make such activity illegal. Professor Clare McGlynn has asserted that the Law Commission's recommendations regarding a new offence image-based abuse should not focus on the motivation of the perpetrator, but recognise instead the threat and invasion of privacy for the victim, which has been endorsed by Glitch, Refuge and other groups.[87] Finally, subsequent codes of practice developed in response to including these types of harms may help address how the existing functionalities and mechanisms of in-scope services might exacerbate the harm caused by VAWG. A joint submission from charities in the VAWG sector, detailing the experience of survivors of VAWG such as image-based sexual abuse, for example, has highlighted to us the need for bespoke codes of practice in this area:

79 Q 67 [Susie Hargreaves]
80 techuk (OSH0075)
81 techuk (OSH0075)
82 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, para 176
83 Ibid.
84 Ibid., paras 179–80
85 Importantly, Mrs Miller emphasised that the software used to do this is only targeted at women.
86 Qq 123–4, 130, 148
87 Q 129; Glitch (OSH0013); Professor Clare McGlynn (OSH0034)

> A year later, the content is still online against my wishes. Attempts to get it removed using DMCA takedown notices work for some time, for them to only be reuploaded. Filing for DMCA takedown notices is an issue in itself. It is dangerous to file these notices yourself as they require a name, address and contact details which are then shared with the person who uploaded the content and is then sometimes used for blackmail or doxing.[88]

Following our evidence session on this matter, the Prime Minister, when questioned by our Chair, did commit to incorporate online VAWG such as cyberflashing (as well as content that advocates self-harm, another type of "legal but harmful" content) on the face of the Bill.[89]

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

29. **The Joint Committee on the Draft Online Safety Bill has made several recommendations regarding the Secretary of State's powers. We agree with their recommendations to clarify the power to make exemptions for services in scope and remove the power to modify Codes of Practice and give guidance to Ofcom. However, the Secretary of State's powers when making regulations to designate types of harm should be amended further for legal but harmful content to protect freedom of expression.** ***All regulations making designations under "content that is harmful to children" and "content that is harmful to adults" should be subject to the affirmative procedure. This will provide an important, additional safeguard for freedom of expression, recognising the need for additional parliamentary oversight in this area.***

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

88 #NotYourPorn, Chayn, Dr Fiona Vera Gray, End Violence Against Women Coalition (EVAW), Faith & VAWG Coalition, Glitch, Imkaan, Professor Clare McGlynn, Rape Crisis England & Wales, Refuge, Welsh Women's Aid, Women & Girls Network (WGN), Women's Aid Federation England (OSH0083)

89 Oral evidence taken before the Liaison Committee on 17 November 2021, HC 835, Qq 52–5

3 Enforcing the regime

Ofcom's duties and powers

Transparency and information-gathering powers

31. Fundamentally, the success of the online safety regime relies on an ability to evaluate the role that automated and machine-learning systems and algorithms play in collecting, organising, analysing, predicting, curating, evaluating, recommending and learning from inputs and outputs such as data, signals, content and activity on their services. Recent reports by the Wall Street Journal have revealed that Facebook employees were aware that changes to its algorithm, which more heavily weighed reshared material in the News Feed in an attempt to arrest the decline in user interactions with the service, resulted in a prevalence of "misinformation, toxicity, and violent content" and " unhealthy side effects on important slices of public content, such as politics and news".[90] Marianna Spring told us about an experiment she conducted for Panorama, which highlights the role of algorithms in promoting extreme content:

> We set up a dummy troll account based on accounts that send me abuse so it was predominately engaged in anti-vaccine and conspiracy content but also a small amount of misogyny. It was totally private so it was not sending out abuse to other people, but it was trying to test the algorithms. What we found, after just two weeks, was that on Facebook and Instagram in particular this account, "Barry the troll", was being pushed almost entirely to suggested accounts and pages linked to misogyny, very extreme discussion about rape, harassment, sexual violence and some posts linked to the incel community that Seyi has already mentioned. That was almost all of what was being promoted and suggested by the social media sites.[91]

32. We have heard that there is a need for the Bill to go beyond the current, generic references to Ofcom's powers, set out in provisions in Chapter 3, with respect to assessing algorithms, balanced against the need to safeguard freedom of expression, privacy and propriety of intellectual property. Notably, the Joint Committee has made several welcome recommendations with regards to a specific defence for Ofcom if it receives unsolicited material that would constitute an offence and when handling whistle-blower complaints or evidence of failings in the duty of care where possession of that evidence might itself constitute an offence.[92]

33. Despite this, tech companies have already tried to set the terms of data sharing with Ofcom, couched in pro-privacy terms. As Antigone Davis, Global Head of Safety at Facebook, told the Joint Committee, "One thing that we are quite supportive of, in terms of some of the legislation that we are here to talk about today, is working with regulators to set some parameters around that research that would enable that research and would enable people to have trust in the research that is done with access to our data in a privacy-

90 "Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead.", The Wall Street Journal, 15 September 2021

91 Q 126

92 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, paras 353 and 439

protected way".[93] This has led to concerns from internet service providers (ISPs), who have warned that information requests to adjacent, out-of-scope services should not overburden them and because such information is unlikely to be sufficiently granular.[94] ***We recommend that the Government provide Ofcom with the power to conduct confidential auditing or vetting of a service's systems to assess the operation and outputs in practice (itself or through an independent third party) in Chapter 3 of the Bill. Alongside the power to request generic information about how " content is disseminated by means of a service", the Government should also include in Section 49(b) a non-exhaustive list of specific information that may be requested, subject to non-disclosure, including:***

- ***The provider's objectives and the parameters for a system's outputs, (such as maximising impressions, views, engagement and so on);***
- ***Their metrics for measuring performance and references of success;***
- ***The datasets on which systems are developed, trained and refined, including for profiling, content recommendation, moderation, advertising, decision-making or machine learning purposes;***
- ***How these datasets are acquired, labelled, categorised and used, including who undertakes these tasks;***
- ***Data on and the power to query a system's outputs, including to request or scrape information on said outputs given particular inputs.***

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

Enforcement powers

35. The Government has consistently argued that Ofcom's enforcement powers should go beyond fines, to ensure that systemic failings against the duty of care are not simply seen as a cost of doing business. In the Bill, this includes the power to issue "use of technology notices" (which allow Ofcom to mandate the use of new technology following "persistent and prevalent" failings of the duty of care), business disruption measures (such as service blocking) and a reserve power for the Secretary of State to bring in senior management liability.[95] However, we heard two primary areas of concern for stakeholders regarding these powers: first, legislatively, whether the Bill's provisions provide Ofcom's powers can be used and used proportionately; and second, practically, whether these powers are sufficiently future-proofed.

36. The use of technology power in particular was critiqued both for its potential impracticality as drafted in legislation and for its lack of future-proofing. As the NSPCC's Andy Burrows described:

93 Oral evidence taken before the Joint Committee on the Draft Online Safety Bill on 28 October 2021, HC 609, Q 200

94 Qq 210 [Till Sommer], 225

95 Draft Online Safety Bill, CP 405, May 2021, clauses 63–9, 90–5

> I think we do have questions about whether the legislation as it is drafted is sufficiently future-proofed. A couple of points that I would touch on. The proposed use of technology warning notices places a Catch-22 on Ofcom that to use those notices it must demonstrate a persistent and prevalent problem when some of the measures that we will be looking to act against take away the capacity to be able to prove that. I do not see how that is resolvable in how the Bill is currently drafted.
>
> Another area where I struggle to see that the legislation is future-proofed as it stands is around the move towards decentralised social networks. We know that Twitter, for example, has established its Bluesky unit to try to work through what a decentralised standard for social networks might look like. There is a risk that whether by accident or by design those types of models engineer away the ability to comply with legislation and at that point that leaves Ofcom with limited measures as to what it does in situations like that. Does that effectively take us to a point where Ofcom has the service blocking powers or nothing? Clearly those service blocking powers for a site like Twitter would raise very significant issues of freedom of expression, if that is the only thing that is left in the tank.[96]

Mr Burrows instead posited as a more proactive and internally-consistent approach for "platforms to risk assess and for Ofcom to have the opportunity to intervene at an earlier point" with reference to whether, through a risk assessment, a service provider had identified risks and taken proportionate measures to address reasonably foreseeable harms.[97] The NSPCC's written submission posited that at minimum "Ofcom should envisage hash scanning, and visual and text based classifiers, as part of its approved set of technologies".[98] Big Brother Watch emphasised a further concern that the Bill did not include adequate guardrails for the power to protect civil liberties like the right to privacy balanced against the need to tackle types of harm.[99]

37. Regarding business disruption measures, the Internet Service Providers' Association (ISPA) has been particularly emphatic about the need for greater clarity and future-proofing. ISPA's written submission states that, while these measures provide an important backstop power and it supports the courts-based process to apply them, there "needs to be a clear process to ensure that [business disruption measure] orders are proportionate, technical feasible and that they can be served on all relevant companies that help the facilitate access to the internet".[100] However, ISPA's evidence notes that the Government has yet to publicly consider the impact of emerging technology on the efficacy of these powers outright. Till Sommer, ISPA's Head of Policy, explained how and why this might happen and the implications for the regime:

96 Q 100; see also NSPCC (OSH0076)
97 Q 113
98 NSPCC (OSH0076)
99 Big Brother Watch (OSH0054)
100 Internet Service Providers' Association (ISPA) (OSH0083)

> Through things like DNS over HTTPS[101] and a lot of other highly complex technical developments, you are getting a broader range of gatekeepers—companies, services and devices—that suddenly influence how you or I access the internet. It looks the same to you and me, you are still typing the same URL into your browser and it still goes via the router, but the traffic is being routed differently. It is partially being encrypted. That means we need to look at a wider range of companies when it comes to things like enforcing the Online Safety Bill. When it comes to access or service restriction orders, we cannot look just at access providers, like we did in the past.[102]

ISPA's submission concludes that "we would like to see greater recognition of this admittedly complex issue in the new online safety framework, e.g. through a greater recognition within safety-by-design principles and a broad application of definitions such as access and ancillary facilities".[103]

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

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

- ***The evidential basis for intervention (including the time period this evidence covers);***
- ***The level of risk and severity of harm that exists on the service and the existing systems used to identify and mitigate or manage these risks;***
- ***The implications for human rights, including freedom of expression and user privacy;***
- ***The cost to the service relative to factors such as its user base and revenue.***

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

- ***Time frames and consultation requirements;***
- ***Due consideration for human rights implications, including the unintended coverage of legal content;***

101 Domain Name System (DNS) over HTTPS, also referred to as DoH. DoH is a protocol to encrypt data between a user's device and the DNS resolver, which is responsible for finding the internet resource (such as a website) that you have entered when browsing online. The aim of DoH is to prevent eavesdropping and manipulation of DNS data and therefore increase privacy and security (such as from Man-in-the-Middle attacks that route you to a malicious destination). A number of tech companies are in the process of implementing DoH in their services.

102 Q 221

103 Internet Service Providers' Association (ISPA) (OSH0083)

- ***Consideration for the costs to services that might be required to enact the measure; and***
- ***Processes for updating consumers.***

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

42. Finally, the Antisemitism Policy Trust has noted that while the Bill details how Ofcom should publish decisions for failures against the duty of care, it provides no such provisions for mandatory breach notices for service providers.[104] Such transparency would theoretically incentivise compliance while providing greater transparency for users of a service when a decision is made by Ofcom. ***We recommend that the Government include a provision in the Bill to mandate publication of a breach notice by a service. This should include details of their breaches against the duty of care and be available to view on the platform.***

Redress and judicial review

43. Evidence to our inquiry has also emphasised that the Bill is silent on matters of judicial review and redress. Lord Puttnam told us that:

> I think the Bill as it stands is an invitation to judicial review. It basically will put Ofcom in an almost impossible position. I particularly would highlight the issue here of personal versus group harms. The personal harm will inevitably, if it is a severe harm, go to some form of class-action suit. They will be supported by a group who will share their concerns.
>
> On the other side of the equation you have these very, very powerful companies. Ofcom will then make a judgment. Either party will then have the ability to appeal and I am not a fan, and I do not think you are, of judge-made laws. So, it is very important—and it is subject to what Dr Dias is saying—that we straighten these things out now or they will be straightened out over a period of 10 or 20 years by the courts. That could bring conflict between Parliament and the courts. We have flirted with that in the past. I would not want Britain to go there. So, it is imperative that we sort it out.
>
> Personally, I would bet a pound to a penny that we will end up going to the group harms not just the personal harms, certainly when it comes to the House of Lords and I would like to think in the Commons. I have said this to officials. I think that it is a major flaw in the Bill.[105]

In her supplementary written evidence, Dr Dias further elucidated on the importance of resolving these matters in the Bill itself, arguing that judicial remedies should remain available to users affected by the dissemination of illegal or harmful content as well as those affected by remedial measures whilst not introducing intermediary liability through

104 Antisemitism Policy Trust (OSH0001)
105 Q 20

the back door.[106] Alongside this, she posits that services should be obligated to give notice of any use of remedial measures by a service provider in order to provide a fair opportunity before Ofcom, super-complaint eligible entities or the judiciary.

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

Parliamentary scrutiny and oversight

45. Parliamentary oversight forms an important check on the powers that will accrue to Ofcom and the Secretary of State. Evidence from individuals and organisations across the piece have in particular raised concerns about the Secretary of State's powers in relation to directing Ofcom, amending the scope of legislation with respect to exemptions to businesses and delegating harms, and so on. The Joint Committee has made some welcome recommendations with respect to these powers. However, we would disagree with the notion that a permanent Joint Committee should be established through primary legislation for several reasons, which we have detailed in letters to the Secretary of State and Leader of the House of Commons.[107] First, this represents a significant departure from convention. Government officials have argued that the Joint Committee on Human Rights (JCHR) and Intelligence and Security Committee (ISC) are precedents; however, the JCHR was not established by the Government through primary legislation but by Parliament, and the ISC is not a parliamentary committee. Second, duplicating our existing constitutional role, through evidence sessions, review of annual reports, pre-appointment hearings and bilateral meetings, in providing ongoing democratic scrutiny of regulators such as Ofcom and ICO may result in competing political pressures on these organisations' strategic objectives. Finally, by virtue of our role scrutinising the Department for Digital, Culture, Media and Sport, we already fulfil the role of scrutinising the work of digital regulators and Secretary of State, considering new developments such as the creation of new technologies, and helping to generate policy solutions in this area. Contrary to assertions that there are "[no committees] with a remit to focus on digital regulation",[108] it is inherent to the digital aspect of our remit, which is reflected in prior work ranging from our predecessors' 2008 Report on *Harmful Content on the Internet and in Video Games* and 2018 and 2019 Reports on *Disinformation and 'fake news'*, *Immersive and Addictive Technology* and *The Online Harms White Paper*, as well as our Reports on *Misinformation in the Covid-19 Infodemic* and *Economics of Music Streaming*. Moreover, we consider it a strength of the select committee system that so

106 Q 1; Dr Talita Dias (OSH0090)

107 Correspondence with the Secretary of State for DCMS re Parliamentary scrutiny of online safety regime, 11 and 22 November 2021; Correspondence with Rt Hon Jacob Rees-Mogg MP, Leader of the House of Commons, re recommendations from the Joint Committee on the Online Safety Bill, 16 December 2021 and 7 January 2022

108 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, para 432

many of our colleagues and sister-committees have contributed their perspectives and solutions in this area: for example, we have hosted and/or guested on the Home Affairs, Science and Technology and Treasury Committees for sessions on digital policy, and anticipate future pre-legislative scrutiny work of the Petitions, Work and Pensions and Women and Equalities Committees. **Parliamentary scrutiny of the ongoing work on the UK's regime for digital regulation by the Department for Digital, Culture, Media and Sport, regulators and associated bodies is vital. However, we consider that this is best serviced by the existing, independent, cross-party select committees and evidenced by the work we have done and will continue to do in this area.** ***We recommend that the Government should scrap any plans to introduce a Joint Committee to oversee online safety and digital regulation.***

Conclusions and recommendations

Pre-legislative scrutiny

1. We are pleased that the Government listened to our calls for pre-legislative scrutiny and decided to publish the Online Safety Bill in draft. We also welcome the recent, comprehensive work by the Joint Committee on the Draft Online Safety Bill, the Treasury Committee and the Lords Communication and Digital Committee and anticipate upcoming Reports from the Petitions Committee (on online abuse) and others. It is also important to note that the online safety regime will form only one part of the UK's framework for digital regulation and we hope that the Government will take a similar, collegiate approach, such as giving time for pre-legislative scrutiny, in these areas. (Paragraph 3)

2. *The Government should provide an update on its work on online advertising and digital markets in response to this Report and publish its responses to the consultations in each of these areas by the time it responds to us in two months' time.* (Paragraph 3)

The duty of care

3. *The Government should redraft the Online Safety Bill to state explicitly that the scope of the framework for addressing "illegal content", which should be subject to the most stringent moderation measures, specifically applies to existing criminal offences, rather than regulatory offences and civil or administrative wrongs.* (Paragraph 10)

4. Though the Bill takes several welcome steps to address harms to children, such as duties to tackle child sexual exploitation and abuse (CSEA), we are concerned about the prevalence of content and activity that are seemingly not captured by the proposed regime. One example of such activity is breadcrumbing, where perpetrators deliberately subvert the thresholds of criminal activity and for content removal by a service provider. (Paragraph 12)

5. *We recommend that the Government respond to our concerns about the risk of content and activity that falls below the threshold of outright criminal activity but nonetheless forms part of the sequence for online CSEA. One starting point should be to reframe the definition of illegal content to explicitly add the need to consider context as a factor, and include explicitly definitions of activity like breadcrumbing, on the face of the Bill.* (Paragraph 12)

6. Proposed amendments to the Draft Bill thus far have been a missed opportunity in making the broader definitions of harm compatible with international human rights law and address societal harms like Covid-19 disinformation. We reiterate our conclusion from a previous Report that doing so is not mutually exclusive. (Paragraph 19)

7. *We recommend that the Government reframes the language around considerations for freedom of expression to incorporate a 'must balance' test so Ofcom can interrogate and assess whether providers have duly balanced their freedom of expression obligations with their decision making.* (Paragraph 19)

8. *We recommend that the Government also reframes the definitions of harmful content and relevant safety duties for content that is harmful to children and content that is harmful to adults, to apply to reasonably foreseeable harms identified in risk assessments, and explicitly add the need to consider context, the position and intentionality of the speaker, the susceptibility of the audience and the content's accuracy. These factors would bring the Bill into line with international human rights law and provide minimum standards against which a provider's actions, systems and processes to tackle harm, including automated or algorithmic content moderation, should be judged.* (Paragraph 20)

9. *The Bill should include non-exhaustive, illustrative lists of preventative and remedial measures beyond takedowns for both illegal and 'legal but harmful' content, proportionate to the risk and severity of harm, to reflect a structured approach to content (referenced in paragraph 9). This could include tagging or labelling, covering, redacting, factchecking, deprioritising, nudging, promoting counter speech, restricting or disabling specific engagement and/or promotional functionalities (such as likes and intra- and cross-platform sharing) and so on.* (Paragraph 21)

10. *We recommend that the definition of content that is harmful to adults should explicitly include content that undermines, or risks undermining, the rights or reputation of others, national security, public order and public health or morals, as also established in international human rights law.* (Paragraph 22)

11. Our definitions also provide meaningful ways to proportionately mitigate the impacts of harms to democracy. (Paragraph 23)

12. *We recommend that, in addition to the factors listed above, the definition for content that is harmful to adults should be further clarified to explicitly account for any intention of electoral interference and voter suppression when considering a speaker's intentionality and the content's accuracy, and account for the content's democratic importance and journalistic nature when considering the content's context.* (Paragraph 23)

13. *The Government should add a new Schedule to the Bill providing at least the most relevant types of illegal content and non-exhaustive illustrative lists of proportionate preventative and remedial measures to mitigate and manage risk. It should also provide, in another new Schedule, a detailed procedure for designating new and/or additional offences that constitute illegal content in the Bill through regulations. Alongside the Bill, the Government should issue example Regulations to illustrate how this process would work and ensure it is done consistently post-implementation.* (Paragraph 25)

14. *We recommend that the Government produce new Schedules detailing procedures for designating, by regulations, content that is harmful to children and content that is harmful to adults. Any regulations designating types of harm should define the harms and provide non-exhaustive illustrative lists of factors and proportionate preventative and remedial measures.* (Paragraph 28)

15. The Joint Committee on the Draft Online Safety Bill has made several recommendations regarding the Secretary of State's powers. We agree with their recommendations to clarify the power to make exemptions for services in scope

and remove the power to modify Codes of Practice and give guidance to Ofcom. However, the Secretary of State's powers when making regulations to designate types of harm should be amended further for legal but harmful content to protect freedom of expression. (Paragraph 29)

16. *All regulations making designations under "content that is harmful to children" and "content that is harmful to adults" should be subject to the affirmative procedure. This will provide an important, additional safeguard for freedom of expression, recognising the need for additional parliamentary oversight in this area.* (Paragraph 29)

17. *We recommend that the Government should take forward the commitments made by the Prime Minister and work with charities, campaign organisations and children's advocacy groups to identify, define and address legal but harmful content, such as content that advocates self-harm and types of online violence against women and girls, that are not currently illegal.* (Paragraph 30)

Enforcing the regime

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

    - *The provider's objectives and the parameters for a system's outputs, (such as maximising impressions, views, engagement and so on*);
    - *Their metrics for measuring performance and references of success;*
    - *The datasets on which systems are developed, trained and refined, including for profiling, content recommendation, moderation, advertising, decision-making or machine learning purposes;*
    - *How these datasets are acquired, labelled, categorised and used, including who undertakes these tasks;*
    - *Data on and the power to query a system's outputs, including to request or scrape information on said outputs given particular inputs.* (Paragraph 33)

19. *We also recommend that the online safety regime should require providers to have designated compliance officers, similar to financial services regulation and which we have advocated previously, in order to bake compliance and safety by design principles into corporate governance and decision-making.* (Paragraph 34)

20. *We recommend that the Government provide greater clarity about the use of enforcement powers contained in the Bill. First, it should make explicit that these powers apply only to in-scope services.* (Paragraph 38)

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

    - *The evidential basis for intervention (including the time period this evidence covers);*
    - *The level of risk and severity of harm that exists on the service and the existing systems used to identify and mitigate or manage these risks;*
    - *The implications for human rights, including freedom of expression and user privacy;*
    - *The cost to the service relative to factors such as its user base and revenue.* (Paragraph 39)

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

    - *Time frames and consultation requirements;*
    - *Due consideration for human rights implications, including the unintended coverage of legal content;*
    - *Consideration for the costs to services that might be required to enact the measure; and*
    - *Processes for updating consumers. (*Paragraph 40*)*

23. *The Government should also give consideration to, and evaluate in its response to this Report, whether these powers are appropriately future-proofed given the advent of technology like VPNs and DNS over HTTPs.* (Paragraph 41)

24. *We recommend that the Government include a provision in the Bill to mandate publication of a breach notice by a service. This should include details of their breaches against the duty of care and be available to view on the platform.* (Paragraph 42)

25. The Government must provide further clarity on the subject of redress and judicial review to ensure the effective implementation of the Online Safety Bill. (Paragraph 44)

26. *We recommend that the Government should include a provision in the Bill to clarify that the right of eligible entities to make super-complaints before Ofcom is without prejudice to the right of individuals to access courts and make judicial complaints on a case-by-case basis for breaches of user-to-user and search service providers' duties of care laid down in the Bill and other acts or omissions that are unlawful under other applicable laws. The Government should amend Clauses 15(3) and 24(3) to impose a duty on providers to operate a complaints procedure that gives users notice of any restriction on their ability to access and use the service, along with the reasons for the restriction.* (Paragraph 44)

27. Parliamentary scrutiny of the ongoing work on the UK's regime for digital regulation by the Department for Digital, Culture, Media and Sport, regulators and associated bodies is vital. However, we consider that this is best serviced by the existing, independent, cross-party select committees and evidenced by the work we have done and will continue to do in this area. (Paragraph 45)

28. *We recommend that the Government should scrap any plans to introduce a Joint Committee to oversee online safety and digital regulation.* (Paragraph 45)

Formal minutes

Thursday 20 January 2022

Members present:

Julian Knight, in the Chair

Clive Efford

Julie Elliott

Rt Hon Damian Green

John Nicolson

Jane Stevenson

The Draft Online Safety Bill and the legal but harmful debate

Draft Report (*The Draft Online Safety Bill and the legal but harmful debate*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 45 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Eighth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No.134.

Adjournment

Adjourned till Tuesday 25 January 2022 at 9.30 am.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Thursday 23 September 2021

The Lord Puttnam CBE, Chair of the Democracy and Digital Technologies Committee; **Professor Alan Renwick**, Professor of Democratic Politics and Deputy Director of the Constitution Unit, University College London; **Dr Talita de Souza Dias**, Shaw Foundation Junior Research Fellow in Law, Jesus College, University of Oxford — Q1–33

Tuesday 26 October 2021

Andy Burrows, Head, Child Safety Online Policy, NSPCC; **Susie Hargreaves OBE**, Chief Executive, Internet Watch Foundation — Q3–117

Seyi Akiwowo, founder and director, Glitch; **Rt Hon Maria Miller MP**; **Marianna Spring**, specialist disinformation and social media reporter, BBC; **Cordelia Tucker O'Sullivan**, Senior Policy and Public Affairs Manager, Refuge — Q118–148

Tuesday 9 November 2021

Lexie Kirkconnell-Kawana, Head of Regulation, IMPRESS; **Michelle Stanistreet**, General Secretary, National Union of Journalists — Q149–203

Iain Corby, Executive Director, Age Verification Providers Association; **Julie Dawson**, Director of Regulatory and Policy, Yoti; **Till Sommer**, Head of Policy, Internet Service Providers Association — Q204–226

Tuesday 14 December 2021

Julie Inman Grant, Australian e-Safety Commissioner — Q227–260

Tuesday 18 January 2022

Iain Bundred, Head of Public Policy UK&I, YouTube; **Richard Earley**, UK Public Policy Manager, Meta; **Elizabeth Kanter**, Director of Government Relations and Public Policy, TikTok; **Niamh McDade**, Deputy Head of UK Policy, Twitter — Q261–298

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

OSH numbers are generated by the evidence processing system and so may not be complete.

1 5Rights Foundation (OSH0019)

2 Adam Smith Institute (OSH0053)

3 Advertising Standards Authority (OSH0010)

4 Age Verification Providers Association (OSH0091)

5 Age Verification Providers Association (OSH0060)

6 Antisemitism Policy Trust (OSH0001)

7 Association of British Insurers (OSH0044)

8 BT Group (OSH0074)

9 Barnardo's (OSH0032)

10 Big Brother Watch (OSH0054)

11 British Horseracing Authority (OSH0058)

12 CEASE UK (OSH0015)

13 Carnegie UK (OSH0087)

14 Centenary Action Group; Glitch; The Traveller Movement; Stonewall; Antisemitism Policy Trust; Jo Cox Foundation; Compassion in Politics; Girlguiding; Inclusion London; and Women's Aid (OSH0014)

15 Chayn (OSH0084)

16 Children's Charities' Coalition on Internet Safety (OSH0071)

17 Community Security Trust (OSH0003)

18 Competition and Markets Authority (OSH0086)

19 DMG Media (OSH0064)

20 Demos (OSH0033)

21 Dias, Dr Talita (OSH0090)

22 Dias, Dr Talita (OSH0006)

23 Department for Digital, Culture, Media and Sport (OSH0079)

24 End the Virus of Racism (OSH0057)

25 End Violence Against Women Coalition (OSH0084)

26 Epilepsy Society (OSH0012)

27 Facebook (OSH0089)

28 Faith and VAWG Coalition (OSH0084)

29 Financial Services Compensation Scheme (FSCS) (OSH0035)

30 Full Fact (OSH0065)

31 Glitch (OSH0013)

32 Glitch (OSH0084)

33 Global Action Plan (OSH0043)
34 Gray, Dr Fiona Vera (OSH0084)
35 Guardian Media Group (OSH0072)
36 Hacked Off (OSH0068)
37 Harrison, Dr David (OSH0002)
38 Home Office (OSH0079)
39 Imkaan (OSH0084)
40 IMPRESS: The Independent Monitor for the Press (OSH0008)
41 ISBA (OSH0052)
42 ITV plc (OSH0081)
43 Independent Media Association (OSH0078)
44 Index on Censorship (OSH0029)
45 Institute for the Future of Work (OSH0050)
46 Internet Service Providers' Association (ISPA) (OSH0083)
47 Internet Watch Foundation (OSH0088)
48 Investment Association (OSH0049)
49 LGB Alliance (OSH0070)
50 LGBT Foundation (OSH0031)
51 Legal to Say, Legal to Type (OSH0042)
52 Match Group (OSH0038)
53 McGlynn, Professor Clare (OSH0034)
54 McGlynn, Professor Clare (OSH0084)
55 McGlynn, Professor Clare, (OSH0092)
56 Mencap (OSH0027)
57 Mobile UK (OSH0028)
58 Money and Mental Health Policy Institute (OSH0011)
59 Mumsnet (OSH0030)
60 National Union of Journalists (NUJ) (OSH0026)
61 #Not Your Porn (OSH0084)
62 NSPCC (OSH0076)
63 News Media Association (OSH0069)
64 Nuffield Council on Bioethics (OSH0077)
65 Office of the City Remembrancer, City of London Corporation (OSH0066)
66 Open Rights Group (OSH0039)
67 Orben, Dr Amy (OSH0004)
68 PLSA (OSH0046)
69 Professional Jockeys Association (OSH0058)
70 Professional Players Federation (OSH0005)

71 Rape Crisis (England and Wales)(OSH0084)
72 Renwick, Professor Alan (OSH0040)
73 RSA (OSH0047)
74 Reform Political Advertising (OSH0045)
75 Refuge (OSH0041)
76 Refuge (OSH0084)
77 Reset (OSH0024)
78 Revolut (OSH0067)
79 SafeCast Limited (OSH0023)
80 Stonewall (OSH0017)
81 TSB Bank (OSH0063)
82 The Alan Turing Institute, Public Policy Programme (OSH0007)
83 The Coalition for a Digital Economy (Coadec) (OSH0021)
84 Trustpilot (OSH0037)
85 Twitter (OSH0025)
86 UK Finance (OSH0051)
87 Virgin Media O2 (OSH0062)
88 Walker, Alex (OSH0040)
89 WebGroup Czech Republic, a.s. (formerly WGCZ s.r.o.) and NKL Associates s.r.o (OSH0061)
90 Welsh Women's Aid (OSH0084)
91 Who Targets Me (OSH0055)
92 Women and Girls Network (WGN) (OSH0084)
93 Women's Aid Federation of England (OSH0084)
94 Yoti (OSH0073)
95 techUK (OSH0075)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2021–22

Number	Title	Reference
1st	The future of UK music festivals	HC 49
2nd	Pre-appointment hearing for Information Commissioner	HC 260
3rd	Concussion in sport	HC 46
4th	Sport in our communities	HC 45
5th	Pre-appointment hearing for Information Commissioner	HC 260
6th	Pre-appointment hearing for Chair of the Charity Commission	HC 261
7th	Racism in cricket	HC 1001
1st Special Report	The future of public service broadcasting: Government Response to Committee's Sixth Report of Session 2019–21	HC 273
2nd Special Report	Economics of music streaming: Government and Competition and Markets Authority Responses to Committee's Second Report	HC 719
3rd Special Report	Sport in our communities: Government Response to Committee's Fourth Report	HC 761
4th Special Report	The future of public service broadcasting: Ofcom Response to Committee's Sixth Report of Session 2019–21	HC 832

Session 2019–21

Number	Title	Reference
1st	The Covid-19 crisis and charities	HC 281
2nd	Misinformation in the COVID-19 Infodemic	HC 234
3rd	Impact of COVID-19 on DCMS sectors: First Report	HC 291
4th	Broadband and the road to 5G	HC 153
5th	Pre-appointment hearing for Chair of the BBC	HC 1119
6th	The future of public service broadcasting	HC 156
1st Special Report	BBC Annual Report and Accounts 2018–19: TV licences for over 75s Government and the BBC's Responses to the Committee's Sixteenth Report of Session 2017–19	HC 98
2nd Special Report	The Covid-19 crisis and charities: Government Response to the Committee's First Report of Session 2019–21	HC 438

Number	Title	Reference
3rd Special Report	Impact of Covid-19 on DCMS sectors: First Report: Government Response to Committee's Third Report of Session 2019–21	HC 885
4th Special Report	Misinformation in the COVID-19 Infodemic: Government Response to the Committee's Second Report	HC 894