House of Commons Library

Research Briefing

By John Woodhouse

15 March 2022

Regulating online harms

Summary

Contributing Authors

Image Credits

Social media apps by Tracy Le Blanc / image cropped. Licenced under Pexels Licence – no copyright required.

Disclaimer

Feedback

Every effort is made to ensure that the information contained in these publicly available briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

Contents

Summary

Harmful online content and activity can include cyberbullying, racism, misogynistic abuse, pornography, and material promoting violence and self-harm. Social media platforms have been used to spread anti-vaccine disinformation during the Covid-19 pandemic.

Critics, including parliamentary committees, academics, and children's charities, have argued that self-regulation by internet companies is not enough to keep users safe and that statutory regulation should be introduced.

The Online Harms White Paper (April 2019)

An Online Harms White Paper (April 2019) argued that existing regulatory and voluntary initiatives had "not gone far or fast enough" to keep users safe. The Paper proposed a single regulatory framework to tackle a range of harms. At its core would be a duty of care for internet companies. An independent regulator would oversee and enforce compliance with the duty. A consultation on the proposals closed in July 2019.

The White Paper received a mixed reaction. Children's charities were positive. However, some commentators raised concerns that harms were insufficiently defined. The Open Rights Group and the Index on Censorship warned that the proposals could threaten freedom of expression.

Government response to the White Paper consultation (December 2020)

A full Government response to the White Paper was published in December 2020. This confirmed that an Online Safety Bill would be introduced to impose duties on content-sharing platforms and search services to keep users safe. Ofcom would be the regulator.

Draft Online Safety Bill (May 2021)

A draft Online Safety Bill was included in the Queen's Speech of 11 May 2021. The draft Bill was published the following day, along with Explanatory Notes, an Impact Assessment and a Delegated Powers Memorandum.

Pre-legislative scrutiny

A Joint Committee of both Houses was established in July 2021 to scrutinise the draft Bill. The Committee's report was published on 14 December 2021. This said that the Bill was a "a key step forward" in bringing "accountability and responsibility to the internet". However, the Committee argued that the

Bill should be restructured so that its objectives were clear from the beginning.

The Committee put forward what it referred to as a "cohesive set of recommendations" to strengthen the forthcoming legislation. These included agreeing with Law Commission recommendations on new communications offences. The Committee also recommended that:

- all pornography sites should have duties to stop children from accessing them, regardless of whether the sites hosted user-to-user content.
- individual users should be able to complain to an Ombudsman when platforms failed to comply with their obligations.
- a senior manager should be designated as the "safety controller" with liability for a new offence – failing to comply with their obligations when there was clear evidence of repeated and systemic failings that resulted in a significant risk of serious harm to users.

Other select committee reports

The draft Bill has also been examined in the following reports:

- Petitions Committee, Tackling Online Abuse, February 2022
- Treasury Committee, Economic Harm, February 2022
- Digital, Culture, Media and Sport Committee, The Draft Online Safety Bill and the legal but harmful debate, January 2022
- House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age, July 2021

February/March 2022: Government announces changes to the forthcoming Bill

The Government has said that the Online Safety Bill will be introduced "as soon as possible". In February and March 2022, the Government announced changes to the forthcoming Bill.

Communications offences

On 4 February, the DCMS announced that it was accepting the Law Commission's recommendations for a harm-based communications offence, a false communications offence, and a threatening communications offence. These would be brought into law through the Bill. The Government was considering the Commission's other recommendations for offences relating to cyberflashing, hoax calls, encouraging or assisting self-harm, and epilepsy trolling.

Priority offences

On 7 February, the DCMS announced that it would be setting out further priority offences on the face of the Bill (offences relating to terrorism and child sexual abuse and exploitation are already listed). This was in response to recommendations from the Joint Committee on the draft Bill, the DCMS Committee and the Petitions Committee.

The offences would include incitement to and threats of violence, hate crime, and financial crime. Listing these offences in the Bill would mean that companies would not have to wait for secondary legislation before taking proactive steps to tackle priority illegal content.

Protecting children from pornography

On 8 February, the DCMS announced that the Bill would be strengthened so that all providers who published or placed pornographic content on their services would need to prevent children from accessing that content. This was in response to concerns that non-user generated pornography was not within the scope of the draft Bill.

Online abuse

On 25 February, the DCMS announced that, to tackle online abuse, including anonymous abuse, the Bill would impose two additional duties on category 1 service providers (i.e. the largest platforms):

- a "user verification duty" would require category 1 providers to give adult users an option to verify their identity. Ofcom would publish guidance setting out how companies could fulfil the duty and the verification options that companies could use.

- a "user empowerment tools duty" would require category 1 providers to give adults tools to control who they interacted with and the legal content they could see.

The new duties are in response to concerns raised by the Joint Committee on the draft Bill, the DCMS Committee, and the Petitions Committee about the impact of abuse and the need to give users more control over who they interacted with.

Paid-for fraudulent adverts

On 9 March, the DCMS announced that category 1 service providers and search services would have a duty to prevent the publication of paid-for fraudulent adverts. This was in response to recommendations from the Joint Committee on the draft Bill, the DCMS Committee and others.

The Government also announced a separate Consultation on the Online Advertising Programme. This would complement the Bill and would seek views on improving transparency and accountability across the online advertising supply chain.

Cyberflashing

On 14 March, the DCMS announced that the Bill would create a new criminal offence relating to "cyberflashing". This would be constructed as recommended by the Law Commission. A new section 66A would be inserted into the Sexual Offences Act 2003 to criminalise:

> intentionally sending or giving a photograph or film of any person's genitals to another person with the intention that that person will see the genitals and be caused alarm, distress or humiliation, or for the purpose of obtaining sexual gratification and reckless as to whether the recipient will be caused alarm, distress or humiliation.

Related Library Briefing

A selection of comment on the draft Bill is available in the Library Paper, Reaction to the draft Online Safety Bill: a reading list.

1 Background

The criminal law applies to online activity in the same way as to offline activity. A range of offences can cover offensive online communications including sexual offences, public order offences, and stalking and harassment. There are also specific communications offences prohibiting communications that are menacing, grossly offensive, indecent, obscene or false.[1]

Various regulators have a role in relation to some forms of online activity, e.g. the Competition and Markets Authority, the Advertising Standards Authority, the Information Commissioner's Office, and the Financial Conduct Authority.[2] Ofcom can take action against UK-established video sharing platforms that do not adopt measures to protect users from harmful content.[3] The internet is therefore not quite an unregulated "Wild West" as some have claimed.[4] However, there is no overall regulator with responsibility for content.[5]

For material that is harmful, but not illegal, social media platforms self-regulate through "community standards" and "terms of use" that users agree to when joining. This type of content can be indecent, disturbing or misleading. It can also be abusive, violent, and bullying.[6] The Petitions Committee has noted that online abuse can be "disproportionately targeted" at people depending on, for example, their disability, religion, sexuality,

1 For further discussion see: House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age, HL Paper 54, July 2021, chapter 2; Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill, Report of session 2021-22, 14 December 2021, HL Paper 129/ HC 609, chapter 2; Crown Prosecution Service, Guidelines on prosecuting cases involving communications sent via social media, August 2018 [accessed 9 March 2022]

2 House of Lords Select Committee on Communications, Regulating in a digital world HL Paper 299, March 2019, Appendix 4

3 The Government's intention is for VSP regulation to be in place until its online safety regime comes into force. For further detail see: Ofcom website, Regulating video-sharing platforms: what you need to know [accessed 9 March 2022]; PQ response 135927 [on user-generated video], answered 15 January 2021

4 House of Lords Select Committee on Communications, Regulating in a digital world, p9; Science and Technology Committee, Impact of social media and screen-use on young people's health, HC 822, January 2019, p52

5 House of Lords Select Committee on Communications, Regulating in a digital world, p3

6 Chapter 2 of the December 2021 report from the Joint Committee on the draft Online Safety Bill gives an overview of the different types of online harms

ethnic background or gender.[7] The impact on recipients and their families can be "devastating."[8]

The failure of online platforms to satisfactorily tackle harmful content and activity has led to calls for statutory regulation.[9]

Social media companies - a duty of care?

In 2018, Lorna Woods (Professor of Internet Law at the University of Essex) and William Perrin (Trustee of Carnegie UK) proposed a regulatory regime, centred on a statutory duty of care, to reduce online harm. The regime, developed under the aegis of the Carnegie UK Trust, was put forward in a series of blog posts. A "refined" proposal was published in January 2019.[10] According to Woods and Perrin, social media providers should be "seen as responsible for a public space they have created, much as property owners or operators are in the physical world". They explained the duty of care as follows:

> …In the physical world, Parliament has long imposed statutory duties of care upon property owners or occupiers in respect of people using their places, as well as on employers in respect of their employees. Variants of duties of care also exist in other sectors where harm can occur to users or the public. A statutory duty of care is simple, broadly based and largely future-proof. For instance, the duties of care in the 1974 Health and Safety at Work Act still work well today, enforced and with their application kept up to date by a competent regulator. A statutory duty of care focuses on the objective – harm reduction – and leaves the detail of the means to those best placed to come up with solutions in context: the companies who are subject to the duty of care. A statutory duty of care returns the cost of harms to those responsible for them…[11]

Parliament would give the regulator a range of harms to focus on: misogyny, harassment, economic harm, emotional harm, harms to national security, to the judicial process and to democracy.[12] The regime would regulate services that:

- had a strong two-way or multiway communications component.
- displayed user-generated content publicly or to a large member/user audience or group.

7 Petitions Committee, Tackling Online Abuse, HC 766 2021-22, February 2022, paras 13-4 and 39-41
8 Ibid, para 21
9 Chapter 3 of the Petitions Committee report on Tackling Online Abuse looks at the "gaps" in social media platforms' responses to abuse
10 Woods L and Perrin W, Internet harm reduction: an updated proposal, Carnegie UK Trust, January 2019 (accessed 9 March 2022)
11 Ibid
12 ibid

It would cover "reasonably foreseeable harm that occurs to people who are users of a service and reasonably foreseeable harm to people who are not users of a service".[13]

According to Woods and Perrin, the regulator should be an existing one with experience of dealing with global companies (they suggested Ofcom, the UK's communications regulator).[14] Large fines, set as proportion of turnover, would be used to make companies change their behavior.[15]

Criticism

Graham Smith has challenged the idea that social media platforms should be viewed as having responsibilities for a public space, similar to property owners in the physical world:

> …The relationship between a social media platform and its users has some parallels with that between the occupier of a physical space and its visitors.
>
> A physical public place is not, however, a perfect analogy. Duties of care owed by physical occupiers relate to what is done, not said, on their premises. They concern personal injury and damage to property. Such safety-related duties of care are thus about those aspects of physical public spaces that are less like online platforms.
>
> That is not to say that there is no overlap. Some harms that result from online interaction can be fairly described as safety-related. Grooming is an obvious example. However that is not the case for all kinds of harm…[16]

Support

A February 2019 NSPCC report drew heavily on the work of Woods and Perrin and argued for a regulator to enforce a duty of care to protect children on social media.[17]

In a January 2019 report, the House of Commons Science and Technology Committee noted the work of Woods and Perrin.[18] The Committee recommended that a duty of care should be introduced to make social media companies "act with reasonable care to avoid identified harms" to users aged under 18.[19]

Woods and Perrin submitted evidence to the House of Lords Communications and Digital Committee during its inquiry into regulating the

---

13 Ibid

14 Ibid

15 Penalties are issued on a similar basis under the General Data Protection Regulation and the Competition Act

16 Smith G, "Take care with that social media duty of care", Cyberleagle blog, 19 October 2018 (accessed 9 March 2022)

17 NSPCC, Taming the Wild West Web: How to regulate social networks and keep children safe from abuse, February 2019, p1 and chapter 3 (accessed 9 March 2022)

18 House of Commons Science and Technology Committee, Impact of social media and screen-use on young people's health, paras 223-5

19 Ibid, para 228

digital world.[20] The Committee's March 2019 report recommended that a duty of care should be imposed on online services hosting user-generated content. The duty would be enforced by Ofcom.[21]

In its May 2018 response to a consultation on its Internet Safety Strategy, the then Government said that companies needed to do more to manage content and behaviour on their platforms.[22] A white paper would be published that would look at increasing the liability of social media platforms for harmful and illegal content.[23]

20 See House of Lords Communications and Digital Committee, Regulating in a digital world, paras 198-202
21 Ibid, paras 205-6
22 HM Government, Response to the Internet Safety Strategy Green Paper, May 2018, p13
23 Ibid, pp15-6

2 Online Harms White Paper (April 2019)

An Online Harms White Paper was published in April 2019. This claimed that the existing "patchwork of regulation and voluntary initiatives" had not gone far or fast enough to keep UK users safe. The White Paper therefore proposed a single regulatory framework to tackle a range of online harms.[24] The core of this would be a new statutory duty of care for internet companies, including social media platforms. An independent regulator would oversee and enforce compliance with the duty. The Paper covered three categories of harms:

- harms with a clear definition.
- harms with a less clear definition.
- underage exposure to legal content.[25]

Part 1 of the Paper gave further detail on the above categories.

The regulatory model

Parts 2 and 3 of the White Paper set out the Government's plans for the regulatory framework.

What would the duty require?

The duty of care would require companies to take greater responsibility for the safety of their users and to tackle the harms caused by content or activity on their services. The regulator would issue codes of practice setting out how to do this. For terrorist activity or child sexual exploitation and abuse (CSEA), the Home Secretary would sign off the codes.

Section 7 of the Paper set out specific areas that codes of practice would be expected to cover: CSEA, terrorism, serious violence, hate crime, harassment, disinformation, encouraging self-harm and suicide, the abuse of public figures, cyberbullying, and children accessing inappropriate content.

Who would the duty apply to?

The White Paper noted that harmful content and behaviour originates from a range of online platforms or services and that these cannot easily be categorised by reference to a single business model or sector. It therefore focused on the services provided by companies. According to the Paper,

24 HM Government, Online Harms White Paper, April 2019, p30

25 Examples of harms in each category were set out in a table on p31 of the White Paper

there were two main types of online activity that can give rise to the online harms in scope:

- hosting, sharing and discovery of user-generated content (e.g. a post on a public forum or the sharing of a video).
- facilitation of public and private online interaction between service users (e.g. instant messaging or comments on posts).

As a wide range of companies and organisations provide the above services, the White Paper's proposals covered social media companies, public discussion forums, retailers that allow users to review products online, non-profit organisations, file sharing sites and cloud hosting providers.[26]

The Paper said that users should be protected from harmful behaviour and content in private as well as public online space. Given the importance of privacy, the framework would "ensure a differentiated approach for private communication". The Paper sought views on how 'private' and 'public' should be defined as well on what regulatory requirements should apply to private communication services.[27]

The regulator

An independent regulator would oversee and enforce the new framework. Its role would include issuing codes of practice, setting out what companies would need to do to comply with the duty of care.

The regulator's initial focus would be on companies posing the "biggest and most obvious risk" to users, either because of the size of a service, or because of known harms.[28] Companies would be required to do what was "reasonably practicable" to meet regulatory requirements. This would be enshrined in legislation.[29] The Paper asked whether the regulator should be a new or an existing body with an extended remit.[30]

Enforcement

The core enforcement powers of the regulator would include:

- issuing civil fines for "for proven failures in clearly defined circumstances".
- serving notices to companies alleged to have breached standards and setting a timeframe to respond.

26 HM Government, Online Harms White Paper, p49
27 Ibid, p50
28 Ibid, p54
29 Ibid, p55
30 Ibid, pp57-8

- publishing public notices about the proven failure of companies to comply with standards.[31]

The Paper sought views on other powers – for example, the disruption of business activities, ISP blocking and senior management liability.[32]

2.1 Comment

The White Paper received a mixed response.

Children's charities

According to NSPCC Chief Executive, Peter Wanless, the Paper was a "hugely significant commitment" that could make the UK a "world pioneer in protecting children online".[33] The Children's Charities' Coalition on Internet Safety "applaud[ed]" the Paper and its recognition that self-regulation had failed.[34]

Anne Longfield, the Children's Commissioner for England, said that the problem of harmful content on social media was getting worse and that self-regulation had to end. She called for the new regulator to "have teeth with strong powers to represent children" and for the balance of power to "to decisively shift" away from companies.[35]

Carnegie UK Trust

In a June 2019 summary response, Lorna Woods, William Perrin and Maeve Walsh said that the White Paper was a "significant step in attempts to improve the online environment".[36] However, they raised various concerns. The White Paper's failure to identify an existing body to be the regulator was a "significant weakness". The Paper's distinction between clearly defined and less clearly defined harms was "not helpful" and it was a mistake to exclude economic harm from the framework's scope.

The Trust also said that it could not support the Government drafting some of the codes of practice, even in relation to the most extreme and harmful speech. According to the Trust, the drafting should be the responsibility of Parliament or, "more likely", the independent regulator after consultation

31 Ibid, pp59-60
32 Ibid, p60
33 "Government listens to our Wild West Web campaign and launches White Paper", NSPCC News [online], 8 April 2019 (accessed 9 March 2022)
34 CHIS, Comments on the Online Harms White Paper, July 2019, p1 (accessed 9 March 2022)
35 "What does the Government's Online Harms White Paper mean for children?", Children's Commissioner News [online], 8 April 2019 (accessed 9 March 2022)
36 Woods L et al, The Online Harms White Paper: a summary response, Carnegie UK Trust, 18 June 2019; A full response, including the Trust's responses to the White Paper's questions, was published in June 2019

with the police, the security services, the Crown Prosecution Service and possibly the Home Secretary.

Without "urgent clarification", the Trust said that the Government had "opened itself up to (legitimate) criticism" that its proposed regime was "about moderation, censorship and takedown".

Further criticism of the framework

Other commentators criticised the White Paper's definition of "online harms". Some argued that it risked conflating legal and social issues, while others claimed it could restrict freedom of expression.[37]

The concept of "harm"

Paul Wragg claimed that the Paper moved "awkwardly and confusingly, between criminality and immorality, between commerce and health and safety, between social cohesion and personal development". Wragg argued there was a tension throughout the Paper between questions of law and ethics, between what is illegal and what is unacceptable. According to Wragg, freedom of expression becomes the "obvious casualty" when attempting to prevent harm to users.[38]

Graham Smith also criticised the Paper's "all-encompassing" approach and its "impermissibly vague" concept of harm, including the "nebulous" notion of "harm to society".[39]

Freedom of expression

In a May 2019 Paper, the Open Rights Group (ORG) noted that social media played a "central role in protecting free expression in society" and was of "particular importance for children and young people's expression and access to information".[40] According to ORG, the Government's proposed framework was "unrealistically vast" and a "poor" conceptual approach.[41] In ORG's view, a regulatory scheme should be "explicitly rooted in the international human rights framework". Any policy intervention should be

---

37 See, for example, Edwards H, "Uncharted territory – the UK sets sail towards regulation of 'Online Harms'", Social Media Law Bulletin, 18 April 2019; "The Guardian view on online harms: white paper, grey areas", Guardian [online], 8 April 2019; Goodman E, "The Online Harms White Paper: its approach to disinformation, and the challenges of regulation", Inforrm blog, 13 April 2019; Hurst A, "Tackling misinformation and disinformation online", Inforrm blog, 16 May 2019 (all accessed 9 March 2022)

38 Wragg P, "Tackling online harms: what good is regulation?", Communications Law, Vol 24(2), 2019, pp49-51

39 Smith G, "Users Behaving Badly: the Online Harms White Paper", Cyberleagle blog, 18 April 2019; See also: Smith G, "The Rule of Law and the Online Harms White Paper", Cyberleagle blog, 5 May 2019 (both accessed 9 March 2022)

40 Open Rights Group, Policy responses to Online Harms White Paper, May 2019, p1 (accessed 9 March 2022)

41 Ibid, pp2-3

underpinned "with a clear, objective evidence base which demonstrates that actions are necessary and proportionate".[42]

The Index on Censorship also warned that the White Paper posed "serious risks to freedom of expression online".[43]

Proportionality

According to other critics, attempts to prevent online harm had to be proportionate to the risks. Emma Goodman, for example, observed that protecting the most vulnerable without over-protecting the less vulnerable was a "challenge".[44]

Ashley Hurst argued that the Government "should scale back its ambition to focus on what is illegal and defined, not legal and vague". According to Hurst, the way forward should be focused on technology and education, approaches that were mentioned in the White Paper, but not in enough detail.[45]

A differentiated duty of care?

In a June 2019 paper, Damian Tambini acknowledged some of the criticisms of the White Paper. He said that its proposals could be "significantly damaging for freedom of expression and pluralism". On the other hand, it could be "a proportionate and effective response" to internet harms.[46]

Tambini agreed that social media companies had a duty of care to protect users. He also agreed that there should be a regulator. However, harms were "insufficiently defined" in the White Paper and there was "a blurring of the boundary between illegal and harmful content". In addition, there was a risk of "significant chilling of freedom of expression".[47] According to Tambini, many of the problems with the Paper's approach could be addressed through a "differentiated" duty of care taking into account the "clear distinction between the illegal/clearly defined and the legal/less clearly defined categories of content".[48]

---

42 Ibid, p4

43 Index on Censorship, Online harms proposals pose serious risks to freedom of expression, April 2019 (accessed 9 March 2022)

44 Goodman E, "The Online Harms White Paper: its approach to disinformation, and the challenges of regulation", Inforrm blog, 13 April 2019 (accessed 9 March 2022)

45 Hurst A, "Tackling misinformation and disinformation online", Inforrm blog, 16 May 2019 (accessed 9 March 2022)

46 Tambini D, Reducing Online Harms through a Differentiated Duty of Care: A Response to the Online Harms White Paper, The Foundation for Law, Justice and Society, June 2019 (accessed 9 March 2022)

47 Ibid, p1

48 Ibid, p8

3 Interim response to the White Paper consultation (February 2020)

A consultation on the White Paper's proposals closed on 1 July 2019. There were over 2,400 responses, including from tech companies, academics, think tanks, charities, rights groups, and publishers. The Government's initial response, published in February 2020, said that it was minded to make Ofcom the regulator for online harms. This was because of its "organisational experience, robustness, and experience of delivering challenging, high-profile remits across a range of sectors".[49]

The response indicated the Government's "direction of travel" in areas where concerns had been raised – for example, freedom of expression, businesses within scope, transparency, and protecting children from age-inappropriate content.

[49] DCMS/Home Office, Online Harms White Paper - Initial consultation response, February 2020, "Our response" para 11

4 Full response to the White Paper consultation (December 2020)

The Government published its full response in December 2020. This claimed that the case for "robust regulatory action" continued to grow.[50] It noted that digital technologies had brought "huge benefits" during the Covid-19 pandemic – for example, enabling remote working and helping people to stay in touch with friends and families. However, the pandemic had also highlighted the risks posed by illegal and harmful content:

> Research shows that 47% of children and teens have seen content that they wished they hadn't seen during lockdown. In a month-long period during lockdown, the Internet Watch Foundation and its partners blocked at least 8.8 million attempts by UK internet users to access videos and images of children suffering sexual abuse….

The pandemic had driven a spike in online disinformation[51] and misinformation,[52] with social media the biggest source of false or misleading information about 5G technologies and COVID-19 vaccinations. [53]

The Government's response acknowledged that many of the major social media companies had "moved further and faster than ever before to tackle disinformation and misinformation during the pandemic". However, this had been inconsistent across services. The response confirmed that a duty of care would be introduced. Ofcom would oversee and enforce compliance. According to the Government, its proposed framework, to be introduced through an Online Safety Bill, would "ensure that companies continue to take consistent and transparent action to keep their users safe".[54] A brief overview of how the framework would work is set out below.

Which companies would the framework apply to?

The framework would apply to companies whose services:

- host user-generated content which can be accessed by users in the UK; and/or

50 DCMS/Home Office, Online Harms White Paper: Full government response to the consultation, December 2020, para 6

51 The deliberate creation and dissemination of false and/or manipulated information that is intended to deceive and mislead audiences

52 Inadvertently sharing false information

53 DCMS/Home Office, Online Harms White Paper: Full government response to the consultation, paras 12-3

54 Ibid, para 14

- facilitate public or private online interaction between service users, one or more of whom is in the UK.

It would also apply to search engines. Any in-scope company that provided services to UK users, regardless of where it is based, would have to comply with the framework.

In its initial response, the Government said that business-to-business services would not be in scope. The full response confirmed that services that play a functional role in enabling online activity (e.g. ISPs) would also be exempt from the duty of care. In addition, there would be exemptions for services used internally by businesses, and many low-risk businesses with limited functionality. The Government estimates that under 3% of UK businesses would be within scope of the legislation.[55]

Journalistic content

In response to concerns about media freedom, content published on a newspaper or broadcaster's website would not be in scope. User comments on that content would also be exempted. For journalistic content shared on in-scope services, the Government said there would be "robust protections" for media freedom in the legislation.[56]

What harmful content or activity would the framework apply to?

The Government's response noted that consultation responses raised concerns about the broad range of potential harms in scope of the framework.[57] The legislation would therefore set out a general definition of harmful content and activity i.e. "where it gives rise to a reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals".[58] Priority categories of harmful content, posing the greatest risk to users, would be set out in secondary legislation:

- criminal offences (e.g. child sexual exploitation and abuse, terrorism, hate crime and the sale of illegal drugs and weapons).
- harmful content and activity affecting children (e.g. pornography).
- harmful content and activity that is legal when accessed by adults, but which may be harmful to them (e.g. content about eating disorders, self-harm or suicide).[59]

55 Ibid, paras 19-21 and 1.1 to 1.5
56 Ibid, paras 22-3 and 1.10 to 1.12
57 Ibid, para 2.1
58 Ibid, para 2.2
59 Ibid, paras 2.1 to 2.3

Disinformation and misinformation

The Government's response made clear that the duty of care would apply to disinformation and misinformation that could cause harm to individuals, e.g. anti-vaccination content.[60]

Anonymity

The framework would not put any new limits on online anonymity. However, under the duty of care, companies would be expected to address anonymous online abuse that is illegal through "effective systems and processes". Where companies providing Category 1 services (i.e. "high-risk, high-reach services") prohibited legal but harmful online abuse, they would have to ensure their terms and conditions were clear about how this applied to anonymous abuse.[61]

Harms not in scope

Harms in the following areas would not be in scope:

- intellectual property rights.
- data protection.
- fraud.
- consumer protection law.
- cyber security breaches or hacking.

The framework would not tackle harm through the dark web. According to the Government, a law enforcement response to tackle criminal activity on the dark web was more appropriate.[62]

What action would companies need to take?

Companies in scope would need to prevent user-generated content or activity on their services causing significant physical or psychological harm to individuals. To do this, they would have to assess the risks associated with their services and take reasonable steps to reduce the risks of harms they have identified. The Government's response explained:

> 2.8 The steps a company needs to take will depend, for example, on the risk and severity of harm occurring, the number, age and profile of their users and the company's size. Search engines will need to assess the risk of harm occurring across their entire service. Ofcom will provide guidance specific to search engines regarding regulatory expectations.

60 DCMS/Home Office, Online Harms White Paper: Full government response to the consultation, paras 2.75-2.88
61 Ibid, Box 9
62 Ibid, para 2.4

> 2.9 Companies will fulfil their duty of care by putting in place systems and processes that improve user safety on their services. These systems and processes will include, for example, user tools, content moderation and recommendation procedures. The proposed safety by design framework (detailed in Part 5) will support companies to understand how they can improve user safety through safer service and product design choices.
>
> The framework would not eliminate harm or the risk of harm entirely. Users would therefore be able to report harm and seek redress as well as challenge wrongful takedown and raise concerns about companies' compliance with their duties.
>
> Specific forms of redress would not be mandated by the Government, and companies would not be required to provide financial compensation to users (other than in accordance with any existing legal liability). However, forms of redress could include content removal; sanctions against offending users; reversal of wrongful content removal or sanctions; mediation; or changes to company processes and policies.[63]

Differentiated expectations

The framework would establish differentiated expectations on companies regarding:

- all companies would have to act regarding illegal content and activity.
- all companies would have to assess the likelihood of children accessing their services and provide additional protections if this is likely.
- companies with "Category 1" services would be required to act with regard to legal but harmful content and activity accessed by adults - because services offering extensive functions for sharing content and interacting with large numbers of users pose an increased risk of harm.

The Government said that its approach would "protect freedom of expression and mitigate the risk of disproportionate burdens on small businesses". In addition, it would "address the current mismatch between companies' stated safety policies and many users' experiences online which, due to their scale, is a particular challenge on the largest social media services".

Category 1 services would be for a small group of "high-risk, high-reach services". These would be designated through a three-step process:

1. primary legislation would set out high level factors which lead to significant risk of harm occurring to adults through legal but harmful content, i.e. the size of a service's audience (because harm is more likely to occur on services with larger user bases) and the

[63] Ibid, paras 2.11 to 2.13, hyperlink added to Part 5

functionalities it offers (because certain functionalities, such as the ability to share content widely or contact users anonymously, are more likely to give rise to harm).

2. the Government would determine and publish thresholds for each of the factors. Ofcom would be required to provide non-binding advice on where these thresholds should be set. The final decision on thresholds will lie with the Government.
3. Ofcom would then be required to assess services against these thresholds and publish a register of all those which meet both thresholds.

Companies providing Category 1 services would be required to publish transparency reports about the steps taken to tackle online harms. The Secretary of State for Digital, Culture, Media and Sport would have the power to extend the scope of companies required to publish such reports.[64]

Codes of practice

The processes that companies would need to adopt to fulfil the duty of care would be set out in codes of practice, published by Ofcom after consultation. Companies would need to comply with the codes or be able to demonstrate to Ofcom that an alternative approach was equally effective. Objectives for the codes would be set out in legislation.

An economic impact assessment would have to be published for each code and Ofcom would also have to assess the impact of its proposals on small and micro businesses.[65]

Protecting freedom of expression

As noted earlier, the White Paper's proposals raised concerns about freedom of expression. According to the Government's full response, "robust protections" had been built into the design of duties on companies:

> Companies will be required to consider users' rights, including freedom of expression online, both as part of their risk assessments and when they make decisions on what safety systems and processes to put in place on their services. Regulation will ensure transparent and consistent application of companies' terms and conditions relating to harmful content. This will both empower adult users to keep themselves safe online, and protect freedom of expression by preventing companies from arbitrarily removing content.[66]

In relation to illegal material, there would be "strong safeguards" for freedom of expression to avoid companies "taking an overly risk-averse approach" to its identification and removal:

64 Ibid, paras 27 to 28 and 2.15 to 2.18
65 Ibid, paras 31-2 and 2.48 to 2.53
66 Ibid, para 2.10

> …Companies will be required to consider the impact on and safeguards for users' rights when designing and deploying content moderation systems and processes. This might involve engaging with stakeholders in the development of their content moderation policies, considering the use of appropriate automated tools, and ensuring appropriate training for human moderators. Companies should also take reasonable steps to monitor and evaluate the effectiveness of their systems, including considering the amount of legitimate content that was incorrectly removed
>
> The regulatory framework will also require companies to give users a right to challenge content removal, as an important protection for freedom of expression...[67]

How would Ofcom oversee and enforce the framework?

The primary duty of Ofcom would be to improve the safety of those using online services (as well as non-users who could be directly affected by others' use). Ofcom's role would include:

- setting codes of practice.
- establishing a transparency, trust and accountability framework.
- requiring all in-scope companies to have effective and accessible mechanisms for users to report concerns.[68]

To tackle non-compliance, Ofcom would have the power to issue fines of up to £18 million or 10% of a company's global annual turnover, whichever was higher. It could also take business disruption measures.[69] A statutory appeals route for companies would be established.

Senior management liability

The White Paper sought views on whether senior managers should be personally liable for failures to meet the duty of care. This proposal generated concern with industry highlighting potential negative impacts on the UK tech sector's attractiveness. The Government's response stated that it would reserve the right to introduce criminal sanctions for senior managers who failed to respond fully, accurately, and in a timely manner, to information requests from Ofcom. The power would not be introduced until at least two years after the framework had come into effect.[70]

Costs

Ofcom would cover its costs from industry fees. Only companies above a threshold based on global annual revenue would be required to notify and

67 Ibid, para 2.25
68 Ibid, para 37 and 4.5 to 4.10
69 Ibid, para 4.43 and Box 19
70 Ibid, para 4.49

pay fees. According to the Government, a "large proportion" of in-scope companies would be exempt.[71]

What role would technology, education and awareness play?

The Government's response noted the role of technology in improving safety online (e.g. using artificial intelligence to identify harmful content) and said that a safety by design framework would set out principles and guidance on how companies could design safer online products and services. An online media literacy strategy, building on Ofcom's existing work on media literacy, would also be published.[72]

Safety by design guidance

The Government published Safety by Design Guidance in June 2021.[73] This explains that safety by design is preventative and is "the process of designing an online platform to reduce the risk of harm to those who use it…It considers user safety throughout the development of a service, rather than in response to harms that have occurred".[74]

Online media literacy strategy

An Online Media Strategy was published in July 2021.[75] The Strategy's objective is to "support organisations to undertake media literacy activity in a more coordinated, wide-reaching, and high quality way over the next 3 years".[76]

4.1 Comment

As with the White Paper, reaction to the Government's full response was mixed. Ofcom welcomed its proposed role as regulator.[77]

Anne Longfield, the Children's Commissioner, said she was pleased that the Government would be introducing a duty of care. However, she said it was

71 Ibid, paras 3.21 to 3.24
72 Ibid, paras 40 to 41 and 5.1 to 5.32
73 GOV.UK, Online safety guidance if you own or manage an online platform, June 2021 (accessed 9 March 2022)
74 GOV.UK, Principles of safer online platform design, June 2021 (accessed 9 March 2022)
75 GOV.UK, Online Media Literacy Strategy, July 2021 (accessed 9 March 2022)
76 DCMS, Online Media Literacy Strategy, July 2021, p4 (accessed 9 March 2022)
77 "Ofcom to regulate harmful content online", Ofcom Statement [online], 15 December 2020 (accessed 9 March 2022)

essential that the Online Safety Bill was introduced as soon as possible to keep children safe.[78]

Parliamentary comment

In a December 2020 statement, Julian Knight, the Chair of the Digital, Culture, Media and Sport Committee, welcomed the duty of care.[79] However, he cautioned that "even hefty fines can be small change to tech giants and it's concerning that the prospect of criminal liability would be held as a last resort". Mr Knight also warned "against too narrow a definition of online harms that is unable to respond to new dangers" and questioned how such harms would be proactively monitored.

In a Commons debate on 15 December 2020, Jo Stevens, the then Shadow Secretary of State for Digital, Culture, Media and Sport, noted the length of time the Government had taken to publish its full response. Until the legislation was on the statute book, online harms would continue to "flourish". According to Ms Stevens, the Government's plans were a "missed opportunity", "timid", and "lacked ambition".[80] She also said that the Government had not "done the hard work" of deciding what should be illegal – e.g. on the encouragement or assistance of self-harm. In addition, there were notable absences from the response, such as financial harm and online scams.[81] During the debate, other Members raised concerns over:

- anonymous abuse.
- future-proofing the law so that it would remain effective as new harmful content and activity emerged.
- age assurance to protect children.
- scams and economic crime.

Carnegie UK Trust

In an initial response to the Government's plans, the Carnegie UK Trust said there was "a good deal to be (cautiously) optimistic about".[82] It was "encouraged" that the language in the Government's response mirrored its work on a statutory duty of care. The confirmation that Ofcom would be the independent regulator was welcomed. However, the Trust was disappointed that the Government had ruled out fraud and scams from the framework's scope and that action on misinformation and disinformation in respect of

78 "Response to Government's Online Harms announcement", Children's Commissioner for England News [online], 15 December 2020 (accessed 9 March 2022)
79 "Chair comments on Online Harms legislation", DCMS Committee News, 15 December 2020
80 HC Deb 15 December 2020 cc148-9
81 HC Deb 15 December 2020 c149
82 "Online Harms: Initial Response", Carnegie UK Trust News [online], 15 December 2020 (accessed 9 March 2022)

adults would be limited to that which caused significant physical or psychological harms to individuals.

In addition, the Trust was not convinced that only the biggest companies should be obliged to take action to prevent harms to adults – "it is often on the smallest platforms where the most damaging and abusive behaviour towards and between adults takes place".

Freedom of expression and privacy

In a December 2020 blog, the Open Rights Group argued that the Government's plans continued to threaten freedom of expression and privacy.[83] The Group's concerns related to, among other things, private messaging, legal but harmful content, and journalistic material.

Big Brother Watch and the Index on Censorship also raised concerns about the Government's proposed framework and its consequences on the right to free speech.[84]

A May 2021 paper from the Institute of Economic Affairs criticised the Government's plans on various grounds, including freedom of expression, claiming that "not being able freely to express and receive ideas and information is itself a harm".[85]

The definition of "harm"

The Government's response stated that harmful content and activity would be understood as that which "gives rise to a reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals".[86] Graham Smith noted that this definition went some way in aligning the proposed duty of care more closely with analogous offline duties of care that are specifically safety related.[87] Moreover, it would "tie Ofcom's hands" to some extent in deciding what constitutes harmful speech. However, he pointed to several difficulties including:

- how should "adverse psychological impact" be understood? – "the broader the meaning, the closer we come to a limitation that could mean little or nothing more than being upset or unhappy. The less clear the meaning, the more discretion would be vested in Ofcom to decide what counts as harm, and the more likely that providers

83 Burns H, "Online harms: freedom of expression under threat", ORG blog, 15 December 2020 (accessed 9 March 2022)

84 "Online harms plans threaten the future of freedom of expression", Big Brother Watch [online], 16 December 2020 (accessed 9 March 2022); Index on Censorship Statement, 15 December 2020

85 Hewson V, More harm than good? The perils of regulating online content, Institute of Economic Affairs, May 2021, p23 (accessed 9 March 2022)

86 DCMS/Home Office, Online Harms White Paper: Full government response to the consultation, para 2.2

87 Smith G, "The Online Harms edifice takes shape", Cyberleagle blog, 17 December 2020 (accessed 9 March 2022)

would err on the side of caution in determining what kinds of content or activity are in scope of their duty of care."

- what is the threshold to trigger the duty of care? - "Is it the risk that someone, somewhere, might read something and claim to suffer an adverse psychological impact as a result? Is it a risk gauged according to the notional attributes of a reasonably tolerant hypothetical user, or does the standard of the most easily upset apply? How likely does it have to be that someone might suffer an adverse psychological impact if they read it? Is a reasonably foreseeable, but low, possibility sufficient?"
- would the risk threshold be set out in legislation or left to the discretion of Ofcom?

Smith concluded that the proposed definition of harm set the stage for a proper debate on the limits of a duty of care, the legally protectable nature of personal safety online, and its relationship to freedom of speech – although he claimed that this debate should have taken place since the White Paper was published. Whether the duty should be supervised and enforced by a regulator was, Smith noted, a separate matter.

5 Draft Online Safety Bill (May 2021)

A draft Online Safety Bill was included in the Queen's Speech of 11 May 2021. The draft Bill was published the following day, along with Explanatory Notes, an Impact Assessment and a Delegated Powers Memorandum.[88]

A DCMS/Home Office press release summarised the draft Bill's provisions. According to the press release, these would "put an end to harmful practices" online while protecting freedom of expression and democratic debate.[89]

5.1 How is the draft Bill structured?

The draft Bill contains seven parts:

- Part 1 contains definitions of the services to which the Bill would apply.
- Part 2 sets out the duties that would apply to in-scope services.
- Part 3 sets out obligations in relation to transparency reporting and the payment of fees.
- Part 4 sets out Ofcom's powers and duties, including duties to carry out risk assessments and to maintain a register of categories of services.
- Part 5 provides for the grounds and avenues for appeals against Ofcom's decisions, and for designated bodies to make super-complaints.
- Part 6 provides for the powers of the Secretary of State for Digital, Culture, Media and Sport to issue a statement of strategic priorities and guidance to Ofcom, and to review the Bill's regulatory framework.
- Part 7 contains miscellaneous and general provisions.

88 GOV.UK, Draft Online Safety Bill

89 "Landmark laws to keep children safe, stop racial hate and protect democracy online published", DCMS/Home Office press release, 12 May 2021

The draft Bill would repeal Part 3 of the Digital Economy Act 2017.[90] Part 3 of the 2017 Act requires the commercial providers of online pornography to have age verification arrangements in place to make sure that users are aged 18 years or over. It has never been commenced. The Government has said that Part 3's objectives would be delivered through its wider plans for tackling online harms.[91]

5.2 The draft Bill's proposals

The draft Bill is complex.[92] However, in summary, it would impose obligations on "regulated services" regarding three types of content:

- illegal content.
- content that is harmful to children.
- content that is legal but harmful to adults.

Regulated services would be user-to-user services and search services that have "links" with the UK.[93]

What would service providers have to do?

A service provider's obligations would depend on its category.

All user-to-user services

All user-to-user services would have to:

- conduct an illegal content risk assessment.[94]
- take proportionate steps to mitigate and effectively manage the risks of harm to individuals as identified by the assessment.[95]
- operate a service using proportionate systems and processes to minimise the presence and dissemination of illegal content, the length of time this content is present online, and to swiftly take down illegal content when alerted to its presence.[96]

90 Clause 131

91 See, for example: DCMS Written Statement on Online Harms (HCWS13), 16 October 2019; Paras 2.35 to 2.45 and Box 10 of the Government's December 2020 response to the Online Harms consultation; For background, see the Library Paper Online pornography: age verification (18 October 2019)

92 As noted by the Joint Committee on the draft Online Safety Bill, Draft Online Safety Bill, Report of session 2021-22, 14 December 2021, HL Paper 129/ HC 609, p21

93 Clauses 2 and 3

94 Clause 7

95 Clause 9(2)

96 Clause 9(3)

- specify in terms of service how individuals would be protected from illegal content.[97]
- ensure that terms of service are clear, accessible, and consistently applied.[98]
- have regard to the importance of protecting users' right to freedom of expression and protecting users from unwarranted infringements of privacy when implementing safety policies and procedures.[99]
- operate reporting systems and complaints procedures so that "appropriate action" can be taken.[100]
- Keep written records and review compliance with the relevant duties.[101]

User-to-user services likely to be accessed by children

In addition to the above obligations, user-to-user services likely to be accessed by children would have to:

- conduct a children's risk assessment.[102]
- take proportionate steps to mitigate and effectively manage the risks of harm to children as identified in the assessment and mitigate the impact of harmful content present on the service.[103]
- operate a service using proportionate systems and processes to prevent children from encountering harmful content.[104]
- specify in terms of service how children would be prevented from encountering harmful content.[105]
- ensure that the terms of service are clear, accessible, and consistently applied.[106]

97 Clause 9(4)
98 Clause 9(5)
99 Clause 12(2)
100 Clause 15
101 Clause 16
102 Clauses 7(3) and (4)
103 Clause 10(2)
104 Clause 10(3)
105 Clause 10(4)
106 Clause 10(5)

Category 1 user-to-user services

Category 1 user-to-user services - the largest online platforms[107] - would also have to:

- conduct an adults' risk assessment.[108]
- specify in terms of service how harmful priority content to adults and how other harmful content identified through the assessment would be dealt with.[109]
- ensure that terms of service are clear, accessible and consistently applied.[110]

Under clause 13 of the draft Bill, Category 1 services would have duties to protect "content of democratic importance". Under clause 14, there would be duties to protect "journalistic content".

Search services

The providers of search services would have obligations similar to those set out above for all user-to-user services and services likely to be accessed by children.[111]

Enforcement

The regulator, Ofcom, would prepare codes of practice to help service providers comply with their duties. Ofcom's powers would include:

- issuing technology notices requiring the use of accredited technology to identify and take down terrorist and CSEA content.[112]
- information gathering, through "information notices", to help with its online safety functions. [113]
- issuing enforcement notices setting out what a provider or individual would need to do to comply with the legislation.[114]
- fining non-compliant companies up to £18 million or 10% of annual global turnover.[115]

---

107 "Category 1 threshold conditions" relating to a service's number of users and functionalities would be set out in Regulations made by the Secretary of State for Digital, Culture, Media and Sport (see Schedule 4 of the draft Bill)

108 Clauses 7(6) and (7)

109 Clause 11 (2)

110 Clause 11(3)

111 A useful overview of the draft Bill is given in Wong, B and Ward O, Online Safety Bill: everything you need to know, BurgesSalmon [online], 24 May 2021 (accessed 6 March 2022)

112 Part 4 Chapter 4

113 Part 4 Chapter 5

114 Part 4 Chapter 6

115 Clause 85

- business disruption measures.[116]

Categories of content

As noted above, all regulated services would have to tackle "illegal content" and "content that is harmful to children". Category 1 services would have to address legal content that could harm adults.

What is illegal content?

Clause 41(3) of the draft Bill states that "content consisting of certain words, images, speech or sounds amounts to a relevant offence if the provider of the service has reasonable grounds to believe that":

> (a) the use of the words, images, speech or sounds amounts to a relevant offence,
>
> (b) the use of the words, images, speech or sounds, when taken together with other regulated content present on the service, amounts to a relevant offence, or
>
> (c) the dissemination of the content constitutes a relevant offence.

Relevant offence means:

- terrorism offences.
- child sexual exploitation and abuse offences.
- an offence set out in secondary legislation.
- other offences directed at an individual as the victim.[117]

What is harmful content?

The meaning of harmful content is set out in clauses 45 to 47 of the draft Bill. In summary, "regulated content"[118] would be considered harmful:

- if it is designated in secondary legislation as "primary priority content" that is harmful to children or "priority content" that is harmful to children or adults.
- if a service provider has "reasonable grounds to believe that the nature of the content is such that there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact" on a child or adult of "ordinary sensibilities".
- If a service provider has "reasonable grounds to believe that there is a material risk" of the dissemination of the content "having a

116 Clause 91
117 Clause 41(4)
118 As defined in clause 39

significant adverse physical or psychological impact" on a child or adult of "ordinary sensibilities".[119]

Online scams

One change from the Government's December 2020 White Paper response is that the draft Bill would bring user-generated online scams (e.g. "romance scams" and fake investment opportunities) into the scope of the regulatory framework. For further background, see the Library Paper Consumer protection: online scams.

5.3 Comment

As with the consultation on the Online Harms White Paper, reaction to the draft Bill has been mixed.

Freedom of expression concerns continue to be raised by groups such as the Index on Censorship,[120] Big Brother Watch,[121] and the Open Rights Group.[122] The latter two groups (and others) have also warned that the draft Bill could undermine, and in some cases prohibit, the use of end-to-end encryption. It is claimed that this would remove protections for private citizens and companies' data and put children, and other vulnerable groups, at risk.[123]

Barnardo's welcomed the draft Bill although the charity cautioned that the "devil is in the detail" and said that it would work with Government to make sure the legislation was as effective as possible.[124]

The Samaritans have claimed that the Bill doesn't go far enough to ensure a "suicide-safer internet" because only the largest and most popular platforms would be required to act on content that is legal but harmful to adults – risking the most harmful suicide and self-harm content moving to less prolific sites.[125]

---

119 Clauses 45-7

120 Index on Censorship, Right to type: how the "duty of care" model lacks evidence and will damage free speech, 23 June 2021 (accessed 18 February 2022)

121 "The UK risks becoming a world leader in online censorship", Big Brother Watch blog, 14 May 2021 (accessed 18 February 2022)

122 "Government's Kafkaesque Plans for Regulating Online Speech Is Condemned", Open Rights Group press release [online], 12 May 2021 (accessed 18 February 2022)

123 "Big Brother Watch Signs Open Letter to MPs To Protect End-To-End Encryption", Big Brother Watch News [online], 14 June 2021 (accessed 18 February 2022); "Encryption in The Online Safety Bill", Open Rights Group blog, 20 July 2021 (accessed 18 February 2022)

124 "Barnardo's responds to publication of draft Online Safety Bill", News release [online], 12 May 2021 (accessed 18 February 2022)

125 "Samaritans responds to the draft Online Safety Bill" , News release [online], 12 May 2021 (accessed 18 February 2022)

The Carnegie UK Trust and various select committee reports have examined the draft Bill in detail, as set out in the following sections. Further comment is given in the Library Paper, Reaction to the draft Online Safety Bill: a reading list.

Carnegie UK Trust analysis

In a June 2021 analysis, the Carnegie UK Trust said that the draft Bill had "the potential to develop into an effective, evidence-based framework for the regulation of social media companies and search engines to prevent harm."[126] However, the Trust argued, among other things, that the Bill was too complex, would give too many powers to the Secretary of State, and lacked a process for defining "significant harm".[127]

In November 2021, the Trust published amendments[128] and a revised Online Safety Bill.[129] An accompanying blog explained that the amendments were in response to issues that the Trust and others had raised in evidence to the Joint Committee:

- Reordering of the Bill so that the purpose of the Bill, its objectives, duties of OFCOM, definitions of harm and duties and actions flowing from them are in a logical order. This greatly improves legibility, making the duties easier to comply with and therefore strengthens the Bill.

- Introducing a broader, but still limited definition of harm to address (a) issues mentioned in the original draft Bill that go beyond harms to an individual; and (b) similar matters presented to the Joint Committee.

- A new duty of care that acts as a foundation to strengthen the two focussed duties about illegal content and content harmful to children. The new duty addresses harmful company systems. The foundation duty provides a broad base from which parliament and the regulator can focus on harms of particular concern. Such priority harms are contained in a new Schedule on the face of the Bill, increasing certainty around scope, and should allow a faster start-up of the regime after Royal Assent.

- More flexible powers for the regulator to apply rules in a targeted manner against risk profiles, based on evidence and due process. This removes the need for crude categories of companies based purely on size and the need for a specific adult harm duty. The Bill is therefore greatly simplified and becomes more targeted and effective

126 Carnegie UK Trust, The Draft Online Safety Bill: initial analysis [online], June 2021, p1 (accessed 18 February 2022)

127 Ibid, p1

128 Carnegie UK Trust, Simplifying and strengthening the draft Online Safety Bill – amendments, 10 November 2021 (accessed 18 February 2022)

129 Carnegie UK Trust, Revised Online Safety Bill, November 2021 (accessed 18 February 2022)

- Trimming back the powers of the Secretary of State to bring them in line with international norms.[130]

The blog listed how the amendments would, in the Trust's view, strengthen and simplify the Bill.

Lords Communications and Digital Committee report (July 2021)

The House of Lords Communications and Digital Committee considered the draft Bill in its July 2021 report on freedom of expression in the digital age.[131] The Committee supported the Bill's proposals in relation to the removal of illegal content and said that Ofcom should hold platforms to strict timeframes where content was clearly illegal.[132] However the Committee was critical of, among other things, the draft Bill's proposals in relation to legal content that could be harmful to adults. It also said that the Bill was "inadequate" in protecting children, particularly in relation to pornography.

Protecting children from online pornography

According to the Committee, a "significant proportion of children see pornography unintentionally, impacting their freedom over what they see online".[133] The Committee noted that Part 3 of the Digital Economy Act 2017 would have applied to all pornographic websites, whereas the draft Bill would only apply to search engines and platforms that facilitated user-to-user interaction.[134] It was the Committee's view that the Government's failure to commence Part 3 of the 2017 Act had "severely impacted children" and that the draft Bill "should ensure that all pornographic websites are in scope of the online safety regime and held to the highest standards."[135]

In its October 2021 response to the Committee's report, the DCMS said that protecting children from online pornography was a government priority.[136] However, it recognised that concerns had been raised about protecting children from pornography on services that did not fall within the scope of the draft Bill. The DCMS would use the pre-legislative scrutiny process to explore whether further measures to protect children were required.[137]

---

130 Carnegie UK Trust, The Online Safety Bill – reducing complexity, establishing a foundation duty, 10 November 2021 (accessed 18 February 2022)

131 House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age, HL Paper 54, 22 July 2021, chapter 2

132 Ibid, p3

133 Ibid, para 142

134 Ibid, para 147

135 Ibid, paras 149-50

136 DCMS, Government response to the House of Lords Communications Committee's report on Freedom of Expression in the Digital Age, October 2021, para 40

137 Ibid, para 42. See paras 40-8 for further detail of what the Government's response said on pornography.

Legal content that may be harmful to adults

The Committee criticised the draft Bill's proposals in relation to legal content that could be harmful to adults and the duties, set out in clause 11, that would be imposed on the largest (category 1) platforms. These platforms would have to conduct risk assessments to identify potential risks from legal but harmful content on their services. Terms and conditions would have to set out clearly how platforms would deal with any harms identified, as well as 'priority categories' of harm designated in secondary legislation. The Committee said that this was not the "right approach" and questioned whether the proposals could be "implemented without unjustifiable and unprecedented interference in freedom of expression".[138]

The Committee argued that if a type of content was seriously harmful, it should be defined and criminalised through primary legislation. For legal content that could be objectionable to some people, this should be addressed through regulating the design of platforms, digital citizenship education, and competition regulation.The Committee set out suggestions for redrafting the Bill if the Government did not accept its recommendations.[139]

In its October 2021 response, the DCMS said that its approach to harmful content accessed by adults had been designed to protect freedom of expression and would not require companies to remove legal content. According to the Government, the draft Bill would increase transparency around companies' moderation processes, and ensure they were held to account for consistent enforcement of their terms of service.[140]

Joint Committee on the Draft Bill report (December 2021)

A Joint Committee of both Houses was established in July 2021 to scrutinise the draft Bill.[141] The Committee's report was published on 14 December 2021.[142] This agreed with the Government that self-regulation by internet companies had failed. It said that the draft Bill was a "a key step forward for democratic societies to bring accountability and responsibility to the internet".[143] However, to be successful, the Committee argued that the Bill needed to be clear about its objectives and should be restructured as follows:

---

138 House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age, para 182

139 Ibid, paras 182-3

140 DCMS, Government response to the House of Lords Communications Committee's report on Freedom of Expression in the Digital Age, para 50. See paras 51-67 for further detail of what the Government's response said on harmful content accessed by adults.

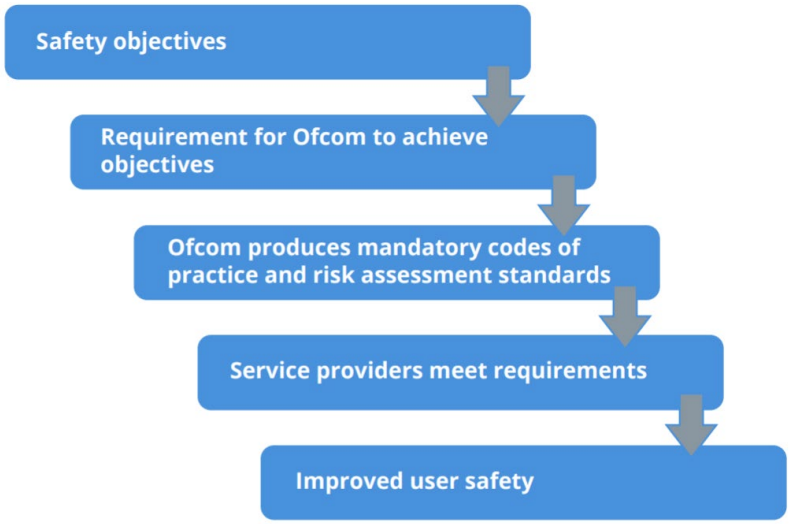
141 "Joint Committee on the Draft Online Safety Bill established", Joint Committee on the draft Online Safety Bill news article [online], 23 July 2021 (accessed 18 February 2022)

142 "No longer the land of the lawless", Joint Committee on the draft Online Safety Bill news article [online], 14 December 2021 (accessed 18 February 2022)

143 Draft Online Safety Bill, Report of session 2021-22, 14 December 2021, HL Paper 129/ HC 609, p3

> …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.[144]

The Committee summarised how the restructured Bill would work in the following figure[145]:



The Committee put forward what it referred to as a "cohesive set of recommendations" to strengthen the forthcoming legislation.[146] These are set out on pages 136-60 of the report. The Committee cautioned that the Government should not "seek to isolate single recommendations without understanding how they fit into the wider manifesto laid out by the Committee". It said that, taken as a whole, the recommendations would help

144 Ibid, para 52
145 Ibid, p25
146 Ibid, para 469

the Government achieve its aim of making the UK the safest place in the world to be online.[147]

The Committee agreed with the Law Commission's recommendations to:

- make cyberflashing illegal.
- make it illegal to deliberately send flashing images to people with photosensitive epilepsy with the intention of inducing a seizure.
- make it illegal to post content or activity promoting self-harm.[148]

The Committee also recommended, among other things, that:

- all pornography sites should have duties to stop children from accessing them, regardless of whether the sites host user-to-user content.[149]
- platforms allowing anonymous and pseudonymous accounts should be required to include the resulting risks as a specific category in the risk assessment on safety by design.[150] Ofcom should 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.[151]
- paid-for advertisements should be brought within the Bill's scope.[152]
- individual users should be able to complain to an ombudsman when platforms failed to comply with their obligations.[153]
- a senior manager should be designated as the "safety controller" with liability for a new offence – failing to comply with their obligations when there was clear evidence of repeated and systemic failings that resulted in a significant risk of serious harm to users.[154]

Legal content that may be harmful to adults

The Committee was critical about the draft Bill's approach to legal content that could be harmful to adults and the duties that it would impose, through clause 11, on Category 1 providers.[155] According to the Committee, the clause had "profound implications" for freedom of speech, could be subject

147 Ibid, p160
148 Ibid, pp141-2
149 Ibid, pp146-7
150 pp29-31 of the report look at safety by design
151 Ibid, pp138-9
152 Ibid, p148
153 Ibid, p159
154 Ibid, p153
155 Ibid, pp51-6

to legal challenge, and could allow some companies to continue in failing to tackle online harm.[156]

The Committee recommended that clause 11 should be removed and 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". The definitions should reference specific areas of law that are recognised in the offline world, or are recognised as legitimate grounds for interference in freedom of expression. The Committee gave the following examples:

- 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.
- Content or activity likely to cause harm amounting to significant psychological distress to a likely audience (defined in line with the Law Commission offence).
- Threatening communications that would lead a reasonable person to fear that the threat might be carried out.
- Knowingly false communications likely to cause significant physical or psychological harm to a reasonable person;
- Unsolicited sending of pictures of genitalia.
- Disinformation that is likely to endanger public health (which may include antivaccination disinformation).
- Content and activity that promotes eating disorders and self-harm.
- Disinformation that is likely to undermine the integrity and probity of electoral systems.[157]

Ofcom would be required to issue a mandatory code of practice to service providers on how they should comply with the duty.

Parliamentary scrutiny and oversight

The Committee said that digital regulation should be subject to "dedicated parliamentary oversight" and recommended that a Joint Committee of both Houses should be established.[158]

156 Ibid, p142
157 Ibid, p143
158 Ibid, p125

Digital, Culture, Media and Sport Committee report (January 2022)

A January 2022 report from the Digital, Culture, Media and Sport Committee considered the draft Bill and the "legal but harmful debate".[159] The report raised "urgent concerns" that the Bill did not adequately protect freedom of expression and was not "clear and robust" enough to tackle certain types of harmful content. The Committee said that such content included "breadcrumbing"[160], a "technically legal" part of child abuse sequences, tech-enabled "nudifying" of women, and deepfake pornography.

Recommendations

The Committee said that the Government should reframe the draft Bill's language around considerations for freedom of expression to incorporate a "must balance" test so that Ofcom could assess whether service providers had balanced their freedom of expression obligations with their decisions about harmful content and activity.[161]

Harmful content

On harmful content, the Committee recommended that the Government should also reframe:

- the definition of illegal content – i.e. to explicitly add the need to consider context as a factor, and include definitions of activity like breadcrumbing, on the face of the Bill.

- the definitions of harmful content and relevant safety duties for content that is harmful to children and content that is harmful to adults – i.e. these should 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.

In addition, the Committee recommended that:

- the Bill should include non-exhaustive, illustrative lists of preventative and remedial measures for both illegal and "legal but harmful" content, proportionate to the risk and severity of harm, to reflect a structured approach to content.[162]

---

159 Digital, Culture, Media and Sport Committee, The Draft Online Safety Bill and the legal but harmful debate, HC 1039 2021-22, 24 January 2022

160 Ibid, para 12 of the Committee's report explains that "breadcrumbing" 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.

161 Ibid, para 19

162 Ibid, para 21

- the definition of content that is harmful to adults should explicitly include content that undermined, or risked undermining, the rights or reputation of others, national security, public order and public health or morals.[163]

- 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.[164]

New schedules should be added to the Bill that would:

- provide the most relevant types of illegal content and non-exhaustive illustrative lists of proportionate preventative and remedial measures to mitigate and manage risk.[165]

- provide a detailed procedure for designating new and/or additional offences that constituted illegal content in the Bill through regulations.[166]

- detail procedures for designating, by regulations, content that is harmful to children and content that is harmful to adults.[167]

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 to provide an additional safeguard for freedom of expression.[168]

Ofcom's duties and powers

According to the Committee, Ofcom's powers were "unclear and impractical".[169] The Committee recommended, among other things, that the Government 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 was proportionate.

163 Ibid, para 22
164 Ibid, para 23
165 Ibid, para 25
166 Ibid, para 25
167 Ibid, para 28
168 Ibid, para 29
169 Ibid, p3

- provide greater clarity on how business disruption measures would work in practice.
- consider whether Ofcom's powers were future-proofed against new technologies.
- mandate the publication of breach notices by service providers.[170]

The Committee also said that service providers should have designated compliance officers, similar to financial services regulation, "to bake compliance and safety by design principles into corporate governance and decision-making".[171]

Parliamentary scrutiny and oversight

The DCMS Committee report disagreed with the recommendation of the Joint Committee on the draft Bill for the establishment of a new Joint Committee to oversee online safety and digital regulation. The report gave three reasons for this:

1. the establishment of such a Committee would represent a "significant departure from convention".
2. duplicating the DCMS Committee's role in providing ongoing scrutiny of regulators (e.g. Ofcom and the Information Commissioner's Office) could result in competing political pressures on these organisations' strategic objectives.
3. the DCMS Committee already scrutinised the work of digital regulators and the Secretary of State, considered new developments, and helped generate policy solutions.[172]

Petitions Committee report (February 2022)

In a February 2022 report on tackling online abuse, the Petitions Committee supported the introduction of a statutory framework to regulate online platforms.[173] However, the Committee called for the Bill to be strengthened, especially in its approach to abuse that was legal but harmful. According to the Committee, there was a lack of clarity on the scope and scale of the content that would be covered. The Committee therefore recommended that the Bill should include as "comprehensive an indication as possible of what content will be covered under its provisions on content that is harmful to adults or to children in the primary legislation".[174]

170 Ibid, paras 39-41
171 Ibid, para 34
172 Ibid, para 45
173 Petitions Committee, Tackling Online Abuse, HC 766 2021-22, 1 February 2022, para 32
174 Ibid, para 38

Communities disproportionately targeted online

According to the Committee, the draft Bill didn't go far enough in acknowledging the link between the characteristics a person may possess (for example, their disability, sexuality, ethnic background or gender) and the risk of facing online abuse.[175] The Committee recommended that the Bill should:

- include a statutory duty for the Government to consult with civil society organisations representing children and users who are most affected by online abuse on the legislation's ongoing effectiveness at tackling online abuse.[176]

- include abuse based on the characteristics protected under the Equality Act and hate crime legislation as priority harmful content in the primary legislation. It should also list hate crime and Violence Against Women and Girls offences as specific relevant offences within the scope of the Bill's illegal content safety duties and specify the particular offences covered under these headings, as the draft Bill already does for terrorism and Child Sexual Exploitation and Abuse offences.[177]

The Committee said that platforms' risk assessments should not treat all users as being equally at risk from abusive content or behaviour. It recommended that platforms should be required to give separate consideration to the different risks faced by groups including women, users from minority ethnic backgrounds, disabled users, and LGBT+ users, and that this requirement should be made explicit in the risk assessment duties set out in the Bill.[178]

Other recommendations

The Committee also recommended, among other things, that:

- the Bill's safety duties relating to content harmful to children should "apply across a sufficiently comprehensive range of platforms" to prevent young people being able to access or encounter harmful content online.[179]

- the Bill should require smaller (i.e. non-category 1) platforms to protect users from content that is legal but harmful to adults.[180]

- social media companies should be fined if they cannot demonstrate to Ofcom that they are preventing people who have been banned for abusive behaviour from setting up new accounts.[181]

---

175 Ibid, paras 39-43
176 Ibid, para 45
177 Ibid, para 46
178 Ibid, para 47
179 Ibid, para 51
180 Ibid, para 55
181 Ibid, para 98

- social media platforms should give users the option to link their account to a form of verified ID on a voluntary basis and block interactions with unverified users, as a way of tackling abuse posted from anonymous or 'throwaway' accounts.[182]

Treasury Committee report (February 2022)

A February 2022 report from the Treasury Committee examined economic crime. Chapter 3 looked at how online platforms are used to promote fraud and what the draft Bill would do in this area. The Committee recommended that the Bill should be amended so that fraudulent content would be designated as "priority illegal content" – meaning that online firms would have to be proactive, rather than reactive, in removing this content from their platforms.[183] The Committee also recommended that fraud via online advertising should be addressed through the Bill.[184]

182 Ibid, para 109
183 Treasury Committee, Economic Harm, HC 145 2021-22, 2 February 2022, para 74
184 Ibid, para 94

6 February/March 2022: Government announces changes to forthcoming Bill

The Government has said that the Online Safety Bill will be introduced "as soon as possible".[185] In February and March 2022, the Government announced changes to the forthcoming Bill.

6.1 Communications offences

In a July 2021 report, Modernising Communications Offences, the Law Commission had recommended a number of new or reformed criminal offences:

- a new "harm-based" communications offence to replace the offences within section 127(1) of the Communications Act 2003 and the Malicious Communications Act 1988.
- a new offence of encouraging or assisting serious self-harm.
- a new offence of cyberflashing.
- new offences of sending knowingly false communications, threatening communications, and making hoax calls to the emergency services, to replace section 127(2) of the Communications Act 2003.[186]

In a Written Ministerial Statement of 4 February 2022, Chris Philp, Minister for Tech and the Digital Economy, announced that the Government was accepting the Commission's recommendations for a harm-based communications offence, a false communications offence, and a threatening communications offence.[187] The offences would be brought into law through the Bill. Mr Philp said they would "help ensure that the criminal law was focused on the most harmful behaviour whilst protecting freedom of expression":

> …The current offences are sufficiently broad in scope that they could constitute a disproportionate interference in the right to freedom of

185 PQ 127388 [on the timetable for the Online Safety Bill], answered 25 February 2022
186 Law Commission website, Reform of the Communications Offences (accessed 18 February 2022)
187 DCMS, Update on the Law Commission's Review of Modernising Communications Offences, Written Ministerial Statement (HCWS 590), 4 February 2022

> expression. The new offences will protect freedom of expression and, in the case of the harm-based offence by increasing the threshold of harm to serious distress, will ensure that communications which individuals find offensive, such as the expression of a view they do not like or agree with, will not be caught. In addition, the court cannot find someone guilty of the harm-based offence or false communications offence if they have a reasonable excuse. A reasonable excuse would include if the communication was or was intended as a contribution to the public interest.
>
> We have also accepted the Law Commission's recommendation to include a press exemption within the general harm-based communications offence and the knowingly false communications offence. Whilst we do not expect the new offences will capture communication made by the media, including this press exemption demonstrates the government's commitment to upholding media freedom.[188]

The existing communications offences would be repealed.

Mr Philip said that the Government was considering the Law Commission's other recommendations for offences relating to cyberflashing, hoax calls, encouraging or assisting self-harm, and epilepsy trolling.

6.2 Priority offences

In a Written Ministerial Statement of 7 February 2022, Mr Philp announced that further priority offences would be set out on the face of the Online Safety Bill.[189] This was in response to the Joint Committee on the draft Bill and the DCMS Committee, who recommended that the most relevant criminal offences should be included in primary legislation. The Petitions Committee had specified several offences that should be listed, including hate crime.

Offences relating to terrorism and child sexual abuse and exploitation are already listed in the Bill. Mr Philp said that offences within the following categories would also be added:

- encouraging or assisting suicide.
- offences relating to sexual images, including revenge and extreme pornography.
- incitement to and threats of violence.
- hate crime.

188 DCMS, Update on the Law Commission's Review of Modernising Communications Offences, Written Ministerial Statement (HCWS 590), 4 February 2022

189 DCMS, Online Safety Update, Written Ministerial Statement (HCWS 593), 7 February 2022

- 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.

Listing the priority offences in the Bill would mean that companies would not have to wait for secondary legislation before taking proactive steps to tackle priority illegal content. For other illegal content, companies would need to have effective systems in place to remove it once it had reported or they became aware of its presence.[190]

6.3 Protecting children from pornography

In a Written Ministerial Statement of 8 February 2022, Chris Philp said that the Government recognised the concern, raised by the Joint Committee on the draft Bill and others, that changes were needed to protect children from pornography on services that did not currently fall within the Bill's scope (i.e. non-user generated pornography). The Government would therefore incorporate a stand-alone provision in the forthcoming Bill that would require providers who published or placed pornographic content on their services to prevent children from accessing that content. According to Mr Philp, this would ensure that all services that would have been captured by part 3 of the Digital Economy Act, and all the user-to-user and search services covered by the Online Safety Bill, would be required to protect children from pornography. The new duty would be enforced by Ofcom.

While the Bill would be technology neutral, companies would be expected to use age verification technologies to prevent children from accessing pornography.[191]

190 Ibid

191 DCMS, Child Online Safety, Written Ministerial Statement (HCWS 599), 8 February 2022

6.4 Online abuse

In a Written Ministerial Statement of 25 February 2022, Chris Philp announced that, to tackle online abuse, including anonymous abuse, the Bill would impose two additional duties on category 1 service providers (i.e. the largest platforms):

- a "user verification duty" would require category 1 providers to give adult users an option to verify their identity. Ofcom would publish guidance setting out how companies could fulfil the duty and the verification options that companies could use.

- a "user empowerment tools duty" would require category 1 providers to give adults tools to control who they interacted with and the legal content they could see.[192]

This was in response to concerns raised by the Joint Committee on the draft Bill, the DCMS Committee, and the Petitions Committee about the impact of abuse and the need to give users more control over who they interacted with.

6.5 Paid-for adverts

In a Written Ministerial Statement of 9 March 2022, Mr Philip announced that category 1 service providers and search services would have a duty to prevent the publication of paid-for fraudulent adverts (e.g. ads with unlicensed financial promotions, fraudsters impersonating legitimate businesses and ads for fake companies).[193] Ofcom would publish Codes of Practice on what companies would need to do to comply with the new duty. This change to the Bill was in response to recommendations from the Joint Committee on the draft Bill, the DCMS Committee and others.

In his Statement, Chris Philp also announced a separate Consultation on the Online Advertising Programme. This would complement the Bill and would seek views on improving transparency and accountability across the online advertising supply chain. Mr Philp explained:

> In relation to fraud specifically, the Online Advertising Programme will address whether other actors in the supply chain, such as intermediaries, have the power and capability to do more. It will focus on the role of intermediaries in onboarding criminal advertisers and facilitating the dissemination of fraudulent content through using the targeting tools

192 DCMS, Online Safety, Written Ministerial Statement (HCWS 640), 25 February 2022

193 DCMS, Online advertising update, Written Ministerial Statement (HCWS 667), 9 March 2022; See also "Major law changes to protect people from scam adverts online", DCMS press release, 9 March 2022

available in the open display market. This will ensure that we close down any vulnerabilities and add defences across the supply chain, leaving no space for criminals to profit.

The Online Advertising Programme's wider objective is to determine whether the current regulatory regime is sufficiently equipped to tackle the challenges posed by the rapid technological developments in online advertising. The consultation identifies a broad range of both illegal and legal harms to consumers, including misleading and offensive content, as well as fraudulent adverts. It also looks at the impact of targeting and placement of adverts and how these practices can exacerbate harmful content for consumers. The roles and responsibilities of all actors involved in the supply chain of online advertising will be considered as part of the consultation.

Any subsequent changes to regulation of online advertising as a result of the consultation will build on the fraud-specific duties in the Online Safety Bill. This will ensure a coherent, comprehensive regulatory framework for all actors across the online advertising supply chain, where individuals are protected from harmful online advertising content, wherever they encounter this.[194]

6.6 Cyberflashing

In a Written Ministerial Statement of 14 March 2022, Chris Philp announced that the Online Safety Bill would create a new criminal offence relating to "cyberflashing" – the non-consensual sending of images of genitals on, for example, dating apps and social media.[195]

Mr Philp explained that the offence would be constructed as recommended by the Law Commission in its report on Modernising Communications Offences. A new section 66A would be inserted into the Sexual Offences Act 2003 to criminalise "intentionally sending or giving a photograph or film of any person's genitals to another person with the intention that that person will see the genitals and be caused alarm, distress or humiliation, or for the purpose of obtaining sexual gratification and reckless as to whether the recipient will be caused alarm, distress or humiliation".[196]

194 DCMS, Online advertising update, Written Ministerial Statement (HCWS 667), 9 March 2022
195 DCMS, Online safety update, Written Ministerial Statement (HCWS 675), 14 March 2022
196 Ibid

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary