House of Commons Library

Research Briefing

By John Woodhouse

8 April 2022

Analysis of the Online Safety Bill

Number 9506

Contributing Authors

Lorraine Conway, Advertising;
Sally Lipscombe, Communications offences; CSEA reporting

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

The Online Safety Bill (PDF) [Bill 285 2021-22] was introduced in the House of Commons on 17 March 2022. Second reading is scheduled for 19 April 2022.

The Government has said the Bill delivers its "manifesto commitment to make the UK the safest place in the world to be online while defending free expression". The Bill has five policy objectives:

- to increase user safety online.
- to preserve and enhance freedom of speech online.
- to improve law enforcement's ability to tackle illegal content online.
- to improve users' ability to keep themselves safe online.
- to improve society's understanding of the harm landscape.

What does the Online Safety Bill do?

The Bill would impose duties on "regulated services" (user-to-user services which share user-generated content (eg Facebook) and search services (eg Google) with "links" to the UK) in relation to three types of content:

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

All regulated services would have to protect users from illegal content. There would be additional duties for services likely to be accessed by children.

All services providing pornographic content would have a duty to prevent children from accessing that material (eg through age verification).

The largest and riskiest Category 1 service providers (such as some social media platforms) would have duties in relation to legal but harmful content to adults. The Bill would also require Category 1 providers to protect democratic debate and journalistic user-generated content.

A duty to prevent fraudulent advertising would be introduced for the largest social media platforms and search engines.

Ofcom would be the independent regulator. It would issue codes of practice recommending measures that service providers could take to comply with

their duties. Ofcom would have enforcement powers including issuing fines of up to £18 million or 10% of a company's worldwide revenue (whichever was higher), as well as business disruption measures.

The Bill would also make changes to existing communications offences, as recommended by the Law Commission.

Where would the Bill take effect?

The Explanatory Notes to the Bill state that, as internet services policy is reserved, the Bill is "broadly reserved". However, a small number of provisions would need legislative consent motions from the devolved administrations.

The Bill's information offences would have extra-territorial application.

Background to the Bill

The Bill represents the culmination of a long process of policy development and consultation. An Internet Safety Strategy Green Paper (PDF) (October 2017) looked at, among other things, the responsibilities of companies to keep users safe and the use of technical solutions to prevent online harms. In May 2018, following a consultation on the Green Paper, the Government announced that it would be publishing a white paper (PDF) setting out plans for online safety legislation.

The Online Harms White Paper (PDF) of April 2019 proposed a new regulatory framework to prevent online harms. At its core would be a duty of care for service providers. A consultation on the proposals closed in July 2019. In its December 2020 response, the Government said that an Online Safety Bill would be introduced.

A draft Online Safety Bill (PDF), published in May 2021, was subject to pre-legislative scrutiny by a Joint Committee of the two Houses of Parliament. The Committee's report (PDF) was published on 14 December 2021. The Government's response (PDF) was published on 17 March 2022 and explains how the Government has incorporated sixty-six of the Committee's recommendations into the Bill. The Government factsheet on the Bill summarises some of the main changes.

Reaction to the Bill

Children's charities, such as Barnardos and Childnet, have welcomed the Bill's provisions on pornography.

However, the End Violence Against Women Coalition has criticised the Government for not naming violence against women and girls as a priority harm on the face of the Bill.

The Government's proposals for tackling content that may be "legal but harmful" to adults have been controversial throughout the policy development leading to the Bill. The provisions in this area remain contentious.

In 2018, the Carnegie UK Trust proposed a duty of care for social media platforms and has followed the development of Government policy since. The Trust welcomed changes that the Government has made in response to scrutiny of the draft Bill but claims, among other things, that the Bill "remains too complex".

The internet lawyer, Graham Smith, has also noted the Bill's length and complexity, and argues it could threaten freedom of expression.

Other commentators, such as Julia Hörnle, Professor of Internet Law at Queen Mary University of London, have said online safety should involve challenging the business models of the largest companies and is about "much more than taking down or blocking harmful content".

Further reaction to the Bill is available in the Library Briefing, The Online Safety Bill: A reading list (PDF).

More on the Bill

The following supporting Government documents have been published:

- Explanatory Notes (PDF).
- Delegated Powers Memorandum (PDF).
- Impact Assessment (PDF).
- Online Safety Bill: European Convention on Human Rights Memorandum.
- Online Safety Bill: Regulatory Policy Committee opinion (PDF).
- Factsheet on the Bill.

1 Introduction

The online world is now central to the way many people connect and communicate, access news and information, and do business. Between 2005 and 2020, the weekly time spent online by UK adults increased from nearly 10 hours to 25 hours.[1] For children (aged 5-15 years) and adults (aged 18-54 years) going online has been described as "almost universal"[2] with 92% of UK internet users communicating online and 82% having a social media profile.[3]

However, the internet can also be misused to threaten, abuse, or incite. According to various research findings referred to by the Department for Digital, Culture, Media and Sport (DCMS):

- 62% of adult internet users have had at least one potentially harmful online experience in the last 12 months. The figure is over 80% for 12 to 15-year-olds.
- in 2020, there were 21.7 million reports of child sexual abuse content online referred to the National Center for Missing and Exploited Children, an increase of 28% from 2019.
- 3% of UK adults and 5% of children aged 12-15 have seen material online promoting terrorism and/or radicalisation.
- in the year ending March 2020, there were 3.7 million instances of fraud in England and Wales, with over half involving the internet.
- nearly one in four people who have experienced a mental health problem have been victim to an online scam, three times the rate among people who have never experienced a mental health problem.
- one study of children between 8-18 years old going to hospital following self-harm found that 26% of them had viewed online self-harm and suicide content.
- at least 51% of children aged 11-13 years old have seen pornography, with much of the viewing being unintentional.

1 Figure quoted in DCMS/Home Office, Online Safety Bill Impact Assessment (PDF), 31 January 2022, p5
2 Ibid, p5
3 Ibid, p5

- one in five children aged 10-15 years in England and Wales experienced at least one type of online bullying behaviour in the year ending March 2020.[4]

The Joint Committee on the draft Online Safety Bill noted the way the largest social media platforms are designed can "facilitate the targeting and amplification of abuse".[5] According to the Committee, the safety of people online is one of the "defining policy issues of our age".[6]

How is online harm currently regulated?

The criminal law applies to online activity in the same way as offline activity. A range of offences can cover offensive online communications including sexual offences, terrorism 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.[7] However, much harmful online content and activity does not cross the threshold of illegality and can include:

- material promoting self-harm and suicide.
- pornography.
- bullying.
- abusive language and threats.
- disinformation (intentionally spreading factually incorrect information) and misinformation (unknowingly spreading factually incorrect information).[8]

4 DCMS/Home Office, Online Safety Bill Impact Assessment (PDF), 31 January 2022, pp5-8

5 Joint Committee on the Draft Online Safety Bill, Report of Session 2021-22 (PDF), HL Paper 129 HC 609, 14 December 2021, p5; For further discussion of the design features and business models of the largest platforms see: House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age (PDF), HL Paper 54 2021-22, July 2021, p3; Hörnle J, "Regulating content won't make the internet safer - we have to change the business models", The Conversation [online], 17 March 2022 (accessed 25 March 2022)

6 Joint Committee on the Draft Online Safety Bill, Report of Session 2021-22 (PDF), HL Paper 129 HC 609, 14 December 2021, p5

7 For further detail and discussion see: House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age (PDF), HL Paper 54, July 2021, chapter 2; Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill (PDF), 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 25 March 2022]

8 Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill (PDF), chapter 2; Digital, Culture, Media and Sport Committee, The Draft Online Safety Bill and the legal but harmful debate (PDF), HC 1039, 24 January 2022, p11; Petitions Committee, Tackling Online Abuse (PDF), HC 766 2021-22, February 2022, chapter 2; House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age (PDF), chapter 2

For content that is harmful, but not illegal, social media platforms self-regulate through "community standards" and "terms of use" that users agree to when joining.

Harmful content can be "disproportionately targeted" at people depending on, for example, their disability, religion, sexuality, ethnic background or gender.[9] The impact of abuse on recipients and their families has been described as "devastating".[10] It can involve anxiety, depression, and suicide. Some users may abandon social media after receiving online abuse.[11]

The failure of some of the larger online platforms to satisfactorily prevent harmful content has led to calls for statutory regulation.[12]

Video sharing platforms

Some user-to-user services – ie UK-established video sharing platforms (VSPs) – are subject to the "VSP regime" set out in Part 4B of the Communications Act 2003. These VSPs must have "appropriate measures" in place to protect users from videos which:

- might impair the physical, mental or moral development of under-18s;
- are likely to incite violence or hatred based on particular grounds such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation; and/or
- directly or indirectly encourage acts of terrorism; show or involve conduct that amounts to child sexual abuse; and show or involve conduct that incites racism or xenophobia.[13]

Ofcom enforces the regime. A list of the VSPs regulated by Ofcom is available and includes platforms such as TikTok and Snap (which owns Snapchat).[14] Ofcom's powers include issuing financial penalties of up to £250,000 or 5%

9 Petitions Committee, Tackling Online Abuse (PDF), HC 766 2021-22, February 2022, paras 13-4 and 39-41; House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age (PDF), paras 32-7

10 Petitions Committee, Tackling Online Abuse (PDF), HC 766 2021-22, February 2022, para 21

11 Petitions Committee, Tackling Online Abuse (PDF), HC 766 2021-22, February 2022, para 16. For further discussion see, for example: Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill (PDF), December 2021, chapter 2

12 Chapter 3 of the Petitions Committee report on Tackling Online Abuse looks at the "gaps" in social media platforms' responses to abuse; See also: House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age (PDF), chapter 2

13 Ofcom website, Regulating video-sharing platforms: what you need to know (accessed 31 March 2022). The Government's intention is for VSP regulation to be in place until its online safety regime comes into force.

14 Ofcom website, Notified video-sharing platforms (accessed 2 April 2022)

of qualifying revenue (whichever is greater). In certain circumstances, Ofcom can suspend and/or restrict a service.

In the Explanatory Notes to the Online Safety Bill, the Government says that, because of the serious harm that online content can cause, "more wide reaching and comprehensive regulation of online services should be introduced".[15] VSPs would then be regulated under this wider framework and Part 4B of the 2003 Act would be repealed.[16]

15 Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, para 9

16 Under clause 170 of the Online Safety Bill

2 Background to the Bill

Much of the debate in recent years has focused on whether social media companies should have a duty of care towards their users. The idea was taken up by the Government in 2019 in its Online Harms White Paper and then in the draft Online Safety Bill of May 2021.

2.1 A duty of care?

The idea of a duty of care was originally developed in 2018-19 by Lorna Woods (Professor of Internet Law at the University of Essex) and William Perrin (Trustee of the Carnegie UK Trust – a wellbeing charity). 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 ".[17] A statutory duty of care would focus on harm reduction and return the cost of harms to those responsible (ie the providers).[18] Woods and Perrin suggested that Ofcom should enforce the proposed framework, with the power to issue fines to make companies change their behavior.

The internet lawyer, 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.[19] However it has proved popular with charities, select committees and government.

Support for a duty of care

A February 2019 NSPCC report drew heavily on the work of Woods and Perrin and called for a duty of care to protect children online.[20]

In a January 2019 report examining the impact of social media on young people, the House of Commons Science and Technology Committee recommended a duty of care should be introduced to make social media

17 Woods L and Perrin W, Internet harm reduction: an updated proposal (PDF), Carnegie UK Trust, January 2019 (accessed 25 March 2022)

18 Ibid

19 Smith G, "Take care with that social media duty of care", Cyberleagle blog, 19 October 2018 (accessed 25 March 2022); Smith's Cyberleagle blog contains a series of posts on the Government's online harms proposals (accessed 25 March 2022). The most recent is "Mapping the Online Safety Bill" , 25 March 2022 (accessed 28 March 2022)

20 NSPCC, Taming the Wild West Web: How to regulate social networks and keep children safe from abuse (PDF), February 2019, p1 and chapter 3 (accessed 25 March 2022)

companies "act with reasonable care to avoid identified harms" to users aged under 18.[21]

A March 2019 report from the House of Lords Select Committee on Communications looked at regulating the digital world. The Committee recommended that a duty of care, to be enforced by Ofcom, should be imposed on online services hosting user-generated content.[22]

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 (PDF). It said a white paper would be published looking at increasing the liability of social media platforms for harmful and illegal content.[23]

2.2 The Online Harms White Paper (April 2019)

An Online Harms White Paper was published in April 2019.[24] 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. 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 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, the Index on Censorship and others warned that the proposals could threaten freedom of expression.

A consultation on the White Paper's proposals closed on 1 July 2019.[25]

Government response (December 2020)

In its February 2020 initial response to the consultation, the Government said it was "minded" to make Ofcom the regulator for online harms. This was

21 House of Commons Science and Technology Committee, Impact of social media and screen-use on young people's health (PDF), HC 822 2017-19, January 2019, paras 228
22 House of Lords Select Committee on Communications, Regulating in a digital world (PDF), HL Paper 299 2019-21, March 2019, p5
23 HM Government, Government response to the Internet Safety Strategy Green Paper (PDF), May 2018, p3
24 HM Government, Online Harms White Paper (PDF), April 2019
25 HM Government, Online Harms White Paper (PDF), April 2019, p30

because of its "organisational experience, robustness, and experience of delivering challenging, high-profile remits across a range of sectors".[26]

The Government's full response to the consultation was published in December 2020.[27] This said the case for "robust regulatory action" continued to grow and that a duty of care would be introduced through an Online Safety Bill. It confirmed Ofcom would be the regulator.

2.3 The 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.

A DCMS and Home Office press release explained what would be required of companies in scope:

> …They will need to consider the risks their sites may pose to the youngest and most vulnerable people and act to protect children from inappropriate content and harmful activity.
>
> They will need to take robust action to tackle illegal abuse, including swift and effective action against hate crimes, harassment and threats directed at individuals and keep their promises to users about their standards.
>
> The largest and most popular social media sites (Category 1 services) will need to act on content that is lawful but still harmful such as abuse that falls below the threshold of a criminal offence, encouragement of self-harm and mis/disinformation. Category 1 platforms will need to state explicitly in their terms and conditions how they will address these legal harms and Ofcom will hold them to account.
>
> The draft Bill contains reserved powers for Ofcom to pursue criminal action against named senior managers whose companies do not comply with Ofcom's requests for information. These will be introduced if tech companies fail to live up to their new responsibilities. A review will take place at least two years after the new regulatory regime is fully operational…[28]

Category 1 services (the largest and highest risk platforms) would have duties to protect "content of democratic importance". There would also be duties to protect "journalistic content".

---

26 DCMS/Home Office, Online Harms White Paper - Initial consultation response, February 2020, para 11

27 DCMS/Home Office, Online Harms White Paper: full government response to the consultation (PDF), CP 354, December 2020, p4

28 Gov.UK, Draft Online Safety Bill; "Landmark laws to keep children safe, stop racial hate and protect democracy online published", DCMS/Home Office press release, 12 May 2021

Ofcom would be given the power to fine non-compliant companies up to £18 million or 10% of annual global turnover, whichever was higher, and have the power to block access to sites.[29]

A selection of comment on the draft Bill is available in the Library Paper, Reaction to the draft Online Safety Bill: a reading list (PDF) (3 March 2022).

Joint Committee on the draft Bill

A Joint Committee of both Houses was established in July 2021 to scrutinise the draft Bill.[30]

In a report published on 14 December 2021, the Committee agreed with the Government that self-regulation by online platforms had failed.[31] The Committee noted the draft Bill had moved from introducing a "singular" or "overarching" duty of care to instead impose duties on service providers "to do particular things" to satisfy Ofcom.[32] According to the Committee, the draft Bill was a "a key step forward for democratic societies to bring accountability and responsibility to the internet".[33] However, it put forward a "cohesive set of recommendations" to strengthen the forthcoming Bill.[34] The Committee agreed with the Law Commission's recommendations to:

- make cyberflashing illegal (sending a photograph or film of a person's genitals to another person).
- 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.[35]

The Committee's many other recommendations[36] included the following:

- all pornography sites should have duties to stop children from accessing them, regardless of whether the sites host user-to-user content.[37]

29 Gov.UK, Draft Online Safety Bill; "Landmark laws to keep children safe, stop racial hate and protect democracy online published", DCMS/Home Office press release [online], 12 May 2021 (accessed 25 March 2022)
30 "Joint Committee on the Draft Online Safety Bill established", Joint Committee on the draft Online Safety Bill news article [online], 23 July 2021 (accessed 25 March 2022)
31 "No longer the land of the lawless", Joint Committee on the draft Online Safety Bill news article [online], 14 December 2021 (accessed 25 March 2022)
32 Draft Online Safety Bill (PDF), Report of session 2021-22, 14 December 2021, HL Paper 129/ HC 609, paras 53-6
33 Draft Online Safety Bill (PDF), Report of session 2021-22, 14 December 2021, HL Paper 129/ HC 609, p3
34 Ibid, para 469
35 Ibid, pp141-2
36 Ibid, pp136-60
37 Ibid, pp146-7

- 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.[38] Ofcom should be required to include proportionate steps to mitigate these risks as part of the mandatory Code of Practice required to ensure safety is built into the design of platforms.[39]

- paid-for advertisements should be brought within the Bill's scope.[40]

- users should be able to complain to an ombudsman when platforms failed to comply with their obligations.[41]

- 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.[42]

Government response

In its March 2022 response to the Committee's report, the Government explained it had incorporated sixty-six of the Committee's recommendations into the Online Safety Bill.[43] The response set out in detail how it had done so.

Damian Collins, Chair of the Joint Committee, said he was "very glad" the Government had adopted so many of the Committee's recommendations and that the Bill was a "huge moment for the safety of all internet users".[44]

Other select committee work

The draft Bill was also examined in the following Committee reports:

- House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age (PDF) (HL Paper 54, 22 July 2021). The Government's response was published on 1 November 2021.[45]

38 pp29-31 of the report look at safety by design
39 Ibid, pp138-9
40 Ibid, p148
41 Ibid, p159
42 Ibid, p153
43 HM Government, Government Response to the Report of the Joint Committee on the Draft Online Safety Bill (PDF), CP 640, 17 March 2022
44 "Government responds to Joint Committee's recommended improvements to Online Safety Bill", Joint Committee on the draft Online Safety Bill news article [online], 17 March 2022 (accessed 25 March 2022)
45 DCMS, Government response to the House of Lords Communications Committee's report on Freedom of Expression in the Digital Age, 1 November 2021

- Digital, Culture, Media and Sport Committee, The Draft Online Safety Bill and the legal but harmful debate (PDF) (HC 1039, 24 January 2022). The Government's response was published on 24 March 2022.[46]

- Petitions Committee, Tackling Online Abuse (PDF) (HC 766 2021-22, 1 February 2022). The Government's response was published on 28 March 2022.

For further discussion of the White Paper, the draft Bill, the select committee reports, and subsequent policy announcements on the Bill, see the Library Paper, Regulating online harms (15 March 2022).

[46] Digital, Culture, Media and Sport Committee, The Draft Online Safety Bill and the legal but harmful debate: Government Response to the Committee's Eighth Report (PDF), Fifth Special Report of Session 2021–22, HC 1221, 24 March 2022

3 The Bill

The Online Safety Bill (PDF) [Bill 285 2021-22] was introduced in the House of Commons on 17 March 2022.[47] The following supporting documents are available:

- Explanatory Notes (PDF).
- Delegated Powers Memorandum (PDF).
- Impact Assessment (PDF).
- Online Safety Bill: European Convention on Human Rights Memorandum
- Online Safety Bill: Regulatory Policy Committee opinion (PDF).

The Bill's policy objectives

The Government has said the Bill delivers its "manifesto commitment to make the UK the safest place in the world to be online while defending free expression".[48] The Bill has five policy objectives:

- to increase user safety online.
- to preserve and enhance freedom of speech online.
- to improve law enforcement's ability to tackle illegal content online.
- to improve users' ability to keep themselves safe online.
- to improve society's understanding of the harm landscape.[49]

What would the Bill do?

The Bill would impose duties on "regulated services" (user-to-user services and search services with "links" to the UK) in relation to three types of content:

47 DCMS, Online Safety, Written Ministerial Statement (HCWS691), 17 March 2022; "World-first online safety laws introduced in Parliament", DCMS press release [online], 17 March 2022 (accessed 25 March 2022)
48 DCMS, Online Safety Bill: factsheet [online], 17 March 2022 (accessed 25 March 2022)
49 DCMS/Home Office, Online Safety Bill Impact Assessment (PDF), 31 January 2022, p1

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

All regulated services would have to protect users from illegal content. There would be additional duties for services likely to be accessed by children.

All services providing pornographic content would have a duty to prevent children from accessing that material (eg through age verification).

The largest service providers would need to implement policies to protect adults from legal but harmful content. They would also have to have measures in place to protect democratic debate and journalistic user-generated content.

A fraudulent advertising duty would be introduced for the largest social media platforms and search engines.

Ofcom would issue codes of practice recommending measures that service providers could take to comply with their duties. The enforcement powers of Ofcom would include issuing fines of up to £18 million or 10% of a company's worldwide revenue (whichever was higher), as well as business disruption measures.

The Bill would also make changes to existing communications offences, as recommended by the Law Commission.

A DCMS factsheet on the Bill summarises what has changed since the draft Bill. It also gives an overview of what the new framework would mean for freedom of expression, journalism, disinformation, racist abuse and anonymity, and protecting women.[50]

Territorial extent within the UK

The Explanatory Notes state that, as internet services policy is reserved, the Bill is "broadly reserved".[51] However, a small number of provisions would need legislative consent motions from the devolved administrations.[52] Annex B to the Explanatory Notes gives further detail on the territorial extent and application of the Bill's provisions.[53]

Remaining chapters of this Briefing

The Bill is broad and complex: it has twelve parts and fourteen schedules. The remaining chapters of this Briefing therefore give an overview of some

50 DCMS, Online Safety Bill: factsheet [online], 17 March 2022 (accessed 25 March 2022)
51 Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, para 39
52 Ibid, para 39
53 Clause 192 of the Bill sets out its territorial extent and application

of the Bill's elements and themes, together with comment from stakeholders. Section 4 considers the services that would be in scope. Sections 5 to 8 examine some of the duties that would apply to **regulated user-to-user services**.

Section 9 looks at the fraudulent advertising duty. Ofcom's duties and powers are summarised in section 10. The Bill's proposals to reform communications offences are discussed in section 11.

For detailed commentary on the Bill's clauses, the reader should consult the Explanatory Notes (PDF).

4 Which services would be in scope?

The Bill defines a "user-to-user service" as an internet service by means of which content that is "generated directly" by a user of the service, or uploaded to or shared on the service, may be encountered by others on that service (**clause 2(1)**).

A "search service" is defined as an internet service which is, or includes, a search engine (**clause 2(4)**).

The Bill would apply to "regulated user-to-user services" and to "regulated search services" (**clause 3**). To be regulated, these services must have links with the United Kingdom (**clause 3(2)(a)**). A service "has links" with the UK if it has:

- a significant number of users in the UK.
- if the UK is a target market.
- if it can be used in the UK by individuals and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK (**clauses 3(5) and (6**).

Schedule 1 sets out when services would be exempt from the Bill's provisions. For example, under **paragraphs 1 to 3**, services would be exempt if the only type of user generated content enabled by the service was email, SMS and/or MMS messages. Under **paragraph 4**, a user-to-user service would be exempt if, among other things, users could only communicate on the service through:

- the posting of comments or reviews on provider content (content published on the service by or on behalf of the service provider).
- the sharing of these comments or reviews on other internet services.

Paragraph 7 would exempt "internal business services".

Paragraph 9 would exempt some user-to-user and search services provided by certain public bodies.

Paragraph 10 provides an exemption for user-to-user or search services provided by education or childcare providers where those services were provided for the purpose of education or childcare.

Internet services providing pornographic content

The providers of internet services on which pornographic content (i.e. pornographic content that is published by a provider and is not user generated) is published or displayed would be within scope (**clause 3(4)(c)**). These providers would need to comply with a duty to ensure that children were not normally able to encounter pornographic content on their services (**clause 68**).

How many companies would be in scope?

According to the Impact Assessment (PDF) on the Bill, about 25,000 platforms would fall within scope of the online safety framework.[54]

4.1 Categories of regulated services and their duties

To "embed proportionality"[55] in the regulatory system, the Bill would create categories of regulated services with differing duties:

- user to user services meeting Category 1 thresholds.
- search services meeting Category 2A thresholds.
- user to user services meeting Category 2B thresholds.

In its Delegated Powers Memorandum, the Government said that Category 1 services would not include search services as it was "not considered appropriate or proportionate for this type of service to have duties in relation to content which is legal and may be accessed by adults".[56]

The thresholds for each category would be set out in secondary legislation (subject to the negative procedure) and would relate to a platform's number of users, its functionalities, and the risk of harm on the platform. **Schedule 10** sets out the procedure for making and amending the regulations. Ofcom would be required to publish a register of each service that met the threshold conditions (**clause 81**).

The Impact Assessment on the Bill explained the likely results of categorising regulated services:

> Category 1 platforms are likely to be the highest risk and highest reach user to user platforms, such as a small group of the largest social media sites and

54 DCMS/Home Office, Online Safety Bill Impact Assessment (PDF), 31 January 2022, p18
55 DCMS/Home Office, Delegated Powers Memorandum on the Online Safety Bill (PDF), 17 March 2022, p89
56 DCMS/Home Office, Delegated Powers Memorandum on the Online Safety Bill (PDF), p89

> pornography sites. The same principle applies to Category 2A but relates to the highest risk and highest reach search services, such as a small group of the largest online search engines. Category 2B services are expected to be high-risk, high reach platforms but that may not necessarily meet the Category 1 threshold. Based on current policy intention, between 30-40 platforms are expected to be designated as either Category 1, 2A, or 2B.[57]

4.2 Differing duties

All regulated user-to-user and search services would have to tackle illegal content. They would also have to assess whether their services were likely to be accessed by children and, if so, protect children from harmful content.

All services providing pornographic content would have a duty to prevent children from accessing that material (eg through age verification).

The largest and riskiest (Category 1) service providers would have duties in relation to legal but harmful content to adults. They would also have to protect democratic debate and journalistic user-generated content.

Category 1 and 2A services would have a fraudulent advertising duty.[58]

Parts 3 to 5 of the Bill set out in full the differing duties that would apply to in scope services.

Requirement to report child sexual exploitation and abuse content

In addition to the duties summarised above, all services in scope would have to put in place systems and processes to ensure that detected but unreported child sexual exploitation and abuse (CSEA) content was reported to the National Crime Agency.

In the Online Harms White Paper, the Government had proposed using a regulatory code of practice to set out guidance on how companies should deal with CSEA content online, including "the reasonable steps companies should take to promptly inform law enforcement where there is information about a CSEA offence".[59]

However, following a consultation on the White Paper, the Government noted calls for a mandatory reporting requirement:

> Stakeholders, including the National Crime Agency and National Centre for Missing and Exploited Children, argued that there should be new, mandatory

57 DCMS/Home Office, Online Safety Bill Impact Assessment (PDF), 31 January 2022, p19

58 For a summary of the differing duties that would apply to services in scope, see Table 2 on pp20-1 of DCMS/Home Office, Online Safety Bill Impact Assessment (PDF), 31 January 2022

59 HM Government, Online Harms White Paper, April 2019, para 7.10

> reporting requirements for child exploitation and sexual abuse content to increase reporting and standardise the approach. In their view, this will improve the ability of law enforcement to tackle child sexual exploitation and abuse offenders and safeguard victims in the UK and elsewhere.[60]

The Government said that it was therefore "minded" to introduce such a requirement. The Government considered that this approach would reflect the seriousness of CSEA and would "ensure that companies provide high quality reports with the information law enforcement need to identify offenders and safeguard victims".[61]

Clause 59 of the Bill would introduce a new mandatory reporting requirement relating to CSEA content. This would build on existing voluntary arrangements for companies to report such content, and the principles set out in the Interim code of practice on online child sexual exploitation and abuse issued by the Government in December 2020 as part of its response to the White Paper consultation.

Under clause 59, UK providers of regulated user-to-user services, regulated search services and combined services would be required to operate the service using systems and processes which secure (so far as possible) that all detected and unreported CSEA content present on the service, or present on websites or databases capable of being searched by the search engine, is reported to the National Crime Agency (NCA).[62]

Non-UK providers of such services would be subject to a similar requirement, but only in respect of UK-linked CSEA content that is not already being reported to overseas law enforcement or an alternative reporting body outside the UK.[63]

Clause 60 would require the Secretary of State to issue regulations regarding reports under clause 59, covering matters such as content, format, timeframes and record-keeping.

Under **clause 62** it would be a criminal offence if, in purported compliance with a clause 59 requirement, a person knowingly or recklessly provides information that is false in a material respect.

The NCA has welcomed the proposed reporting requirement "as it will improve the UK response to the threat, and compel industry to do more to combat child sexual abuse content on their platforms".[64]

---

60 DCMS/Home Office, Online Harms White Paper: full government response to the consultation, December 2020, para 2.70

61 Ibid, para 2.72

62 The NCA leads and coordinates UK law enforcement's response to serious and organised crime, including CSEA, and operates the Child Exploitation and Online Protection (CEOP) command

63 For example the CyberTipline operated by the National Center for Missing & Exploited Children, a US-based non-profit organisation

64 National Crime Agency, New reporting regime for online child sexual abuse content announced, 17 March 2022

4.3 Compliance and codes of practice

Clauses 37(1) and (2) would require Ofcom to issue specific codes of practice in relation to the illegal content duties covering terrorist content and CSEA content. **Clause 37(3)** would require Ofcom to issue codes of practice in relation to providers' other safety duties (as set out in **clause 37(10)**. Under **clause 37(4)** a code of practice would have to published in relation to the fraudulent advertising duties.

Schedule 4 sets out the general principles that Ofcom would have to consider when preparing codes of practice, the online safety objectives, and the measures that could be recommended in codes of practice.

Under **clause 39**, Ofcom would submit a draft code of practice to the Secretary of State and, provided the Secretary of State did not intend to issue a direction to Ofcom (under **clause 40**), the Secretary of State would lay the draft code before Parliament. **Clause 40** would give the Secretary of State the power to direct Ofcom to modify a draft code of practice if the Secretary of State believed that modifications were needed for reasons of public policy or, in respect of the CSEA and terrorism codes, for reasons of national security or public safety. **Clause 41** gives details of the parliamentary procedure for issuing codes of practice following direction by the Secretary of State.

Relationship between duties and codes of practice

Service providers would be treated as complying with their duties if they had followed the recommended measures set out in the relevant codes of practice (**clause 45(1)**). However, providers could take "alternative measures" to comply (**clause 45(5)**).

Effects of codes of practice

A failure by a provider to act in accordance with a provision of a code of practice would not of itself make the provider liable to legal proceedings (**clause 46(1)**). A code of practice would be admissible in evidence in legal proceedings (**clause 46(2)**).

A court or tribunal, when determining a question in legal proceedings, would have to consider a provision of a code of practice that was in force at the time of the question and appeared to the court or tribunal to be relevant (**clause 46(3)**).

Clause 46(4) would place an equivalent requirement on Ofcom when it had to determine a question relating to the exercise of its functions.

4.4 Comment

The UK's technology trade association, techUK, has welcomed the Bill. However, it cautioned that a key test of the Bill's success would be whether it would enable platforms and Ofcom "to make quick and effective decisions":

> [The Bill] can meet this test if it is clear about what it is asking companies to do, if it enhances existing company systems and processes and if it avoids an over- expansion of scope.
>
> The government has recognised that this is a highly complex piece of legislation that seeks to find a delicate balance between sometimes competing objectives.
>
> If we get this balance right, we will have a world-leading system for online content regulation. If we get the balance wrong we will fail citizens and consumers.[65]

In its initial analysis of the Bill (PDF), the Carnegie UK Trust argues against the different categories of services that the Bill would create. According to the Trust, this does not fit with a proportionate or risk-based regime and would not catch harms on fast-growing platforms:

> …very large size itself can be an absolute indicator of risk and using very large size as a proxy brings administrative simplicity, but it is wrong to suppose that smaller size means lower risk. We continue to recommend that categories of providers are removed and risk assessment duties apply across the board.[66]

65 "Online Safety Bill introduced in Parliament", techUK news and views [online], 17 March 2022 (accessed 25 March 2022)

66 Perrin W et al, The Online Safety Bill: Our initial analysis (PDF), Carnegie UK Trust, 30 March 2022 (accessed 2 April 2022), p2

5 Protecting users from illegal content

A key aim of the Bill is to protect users from illegal content. All user-to-user services would need to do so.

5.1 What is illegal content?

Clause 52(2) defines "illegal content" as "content that amounts to a relevant offence". **Clause 52(4)** states that "relevant offence means":

> (a) an offence specified in Schedule 5 (terrorism offences),
>
> (b) an offence specified in Schedule 6 (offences related to child sexual exploitation and abuse),
>
> (c) an offence specified in Schedule 7 (other priority offences), or
>
> (d) an offence, not within paragraph (a), (b) or (c), of which the victim or intended victim is an individual (or individuals).

Clause 52(7) defines priority illegal content as terrorism content, CSEA content, and content that amounts to an offence listed in Schedule 7.

On 7 February 2022, the Government announced that further priority offences would be set out on the face of the Bill.[67] This was in response to the reports from the Joint Committee on the draft Bill,[68] the Digital, Culture, Media and Sport Committee,[69] and the Petitions Committee,[70] which recommended that the most relevant criminal offences should be included in primary legislation. **Schedule 7** of the Bill now includes priority offences in the following areas:

- assisting suicide.
- threats to kill.

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

68 Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill (PDF), December 2021, pp42-4

69 Digital, Culture, Media and Sport Committee, The Draft Online Safety Bill and the legal but harmful debate (PDF), January 2022, pp14-5

70 Petitions Committee, Tackling Online Abuse (PDF), February 2022, pp22-4

- public order offences, harassment, stalking and fear or provocation of violence.
- drug-related offences.
- firearms and weapons offences.
- assisting illegal immigration.
- exploiting prostitutes for gain.
- offences relating to sexual images, including revenge and extreme pornography.
- proceeds of crime.
- fraud.
- financial services.
- inchoate offences.

5.2 What would service providers need to do?

Clause 8 would require all regulated user-to-user services to carry out an "illegal content risk assessment". This would involve, among other things, consideration of:

- the user base.
- the level of risk of users encountering each kind of priority illegal content and other illegal content.
- the level of risk of functionalities of the service facilitating the presence or dissemination of illegal content, identifying and assessing those functionalities that present higher levels of risk.
- how the design and operation of the service could reduce or increase the risks identified.
- Ofcom's risk profiles (**clause 83**) relating to the kind of service it provides.

Ofcom would issue guidance to help service providers carry out their risk assessments (**clause 84**). The findings of the risk assessment would inform the steps a provider would have to take to comply with its safety duties about illegal content (as set out in **clause 9**).

Clause 9 would require a service provider to:

- take or use proportionate measures to effectively mitigate and manage the risks of harm to individuals as identified by the most recent illegal content risk assessment.

- operate a service using proportionate systems and processes designed to:

    - prevent individuals from encountering priority illegal content by means of the service.

    - minimise the length of time for which any priority illegal content is present.

    - where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly take down such content.

Under **clause 9(4)**, the above duties would apply to the way a service was operated and used, as well as to the content present on it. **Clause 9(4)** lists the areas within which a service provider might be required to take or use measures to comply with its illegal content safety duties. These include arrangements for compliance and risk management, service design, policies on access and use, content moderation, user empowerment and support measures and staff policies.[71]

A provider would have to specify in terms of service how individuals would be protected from illegal content, how proactive technology would be used to comply with its duties, and to ensure that terms of service were clear, accessible, and consistently applied (**clauses 9(5) to (8)**).

5.3 Comment

The End Violence Against Women (EVAW) Coalition has criticised the Government for not naming violence against women and girls as a priority harm on the face of the Bill.[72] Andrea Simon, EVAW Director, said that doing so would "set the expectation that tech companies must identify, address and prevent the myriad forms of online abuse that women experience disproportionately". EVAW has launched a petition demanding that the Bill "protects women and girls from online abuse."[73]

The CEO of domestic violence charity Refuge, Ruth Davison, has also said that Refuge's calls for violence against women and girls to be at the heart of

71 Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, para 91

72 "Women and girls failed by government's Online Safety Bill", EVAW news [online], 17 March 2022 (accessed 25 March 2022)

73 Change.org, The UK's new Online Safety Law must protect Women and Girls from Online Abuse (accessed 7 April 2022)

the Bill had "not been heard". Refuge welcomed the Bill tackling "revenge porn", stalking and harassment, but noted these were already crimes covered in existing legislation. The Bill "offered little in the way of new protections" for women and girls".[74]

The Carnegie UK Trust has said that human trafficking offences are a serious omission from Schedule 7.[75]

74 "Refuge responds to the publication of the Online Safety Bill", Refuge press release [online], 17 March 2022 (accessed 25 March 2022)

75 Perrin W et al, The Online Safety Bill: Our initial analysis (PDF), Carnegie UK Trust, 30 March 2022 (accessed 2 April 2022), p2

6 Protecting children

The protection of children is one of the key objectives of the Bill. User-to-user services "likely to be accessed by children" would therefore have additional safety duties.

6.1 What is content that is harmful to children?

Clause 53(4) categorises content that is harmful to children as:

> (a) primary priority content that is harmful to children.
>
> (b) priority content that is harmful to children.
>
> (c) content, not within paragraph (a) or (b), of a kind which presents a material risk of significant harm to an appreciable number of children in the United Kingdom.

Primary priority content and priority content harmful to children would be designated in regulations made the Secretary of State (**clauses 53(2) and (3)** respectively).

Under **clause 55(1)**, the Secretary of State could only designate content as primary priority content if:

> (a) there is a material risk of significant harm to an appreciable number of children presented by content of that description that is regulated user-generated content or search content, and
>
> (b) it is appropriate for the duties set out in sections 11(3)(a) and 26(3)(a) (duty in relation to children of all ages) to apply in relation to content of that description.

Under **clause 55(2)**, the Secretary of State could only designate content as priority content if:

> there is a material risk of significant harm to an appreciable number of children presented by content of that description that is regulated user-generated content or search content.

Ofcom would have to be consulted before any regulations were made (**clause 55(5)**).

6.2 Protecting children from harmful content

Under **clause 10**, services would need to carry out a "children's risk assessment". **Clause 10(6)** lists the factors a service provider would have to consider when carrying out an assessment, for example:

- who the users are likely to be, including the number of users who are children in different age groups.
- the level of risk of harm to children presented by different kinds of content that is harmful to children, giving separate consideration to children in different age groups.
- the level of risk of harmful content which particularly affects individuals with a certain characteristic or members of a certain group.
- the different ways in which the service is used, and the impact of these on the level of risk of harm that might be suffered by children.
- how the design and operation of the service may reduce or increase the risks identified.

Clause 10(5) would require a service provider to notify Ofcom about content they identified as harmful to children which was not specified in secondary legislation as "primary priority" or "priority content that was harmful to children". The provider would also need to inform Ofcom of the incidence of this content on the service.

Clause 11(2) would require a user-to-user service to:

- mitigate and manage the risk of harm to children in different age groups from risks identified in the children's risk assessment carried out under clause 10.
- mitigate the impact of harm to children in different age groups.

Clause 11(3)(a) would require a service provider to use proportionate systems and processes to:

- prevent children of any age from encountering primary priority content (by using, for example, age verification or another means of age assurance).

Clause 11(3)(b) would require a service provider to use proportionate systems and processes to:

- protect children in age groups judged to be at risk from other harmful content (for example, priority content) from encountering it (through age assurance, for example).

6.3 Protecting children from pornography

There were concerns from select committees and other stakeholders that the draft Bill would not protect children from accessing non-user-generated pornography.[76] On 8 February 2022, the Government acknowledged these concerns and announced that the Bill would have a stand-alone provision requiring providers who published or placed pornographic content on their services to prevent children from accessing that content.[77]

Part 5 of the Bill covers pornography. Under **clause 68(2)**, the online providers of regulated pornographic content would have a duty to ensure that children were "not normally able to encounter" this content (for example, by using age verification).

There would also be a duty, under **clause 68(3)**, "to make and keep a written record in an easily understandable form, of":

> (a) the measures taken or in use, and the policies implemented, to comply with the duty set out in subsection (2), and
>
> (b) the way in which the provider, when deciding on and implementing the measures and policies referred to in paragraph (a), has had regard to the importance of protecting United Kingdom users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a regulated service (including, but not limited to, any such provision or rule concerning the processing of personal data).

Ofcom would issue guidance on how to comply with the duties (**clause 69**).

Clause 171 of the Bill would repeal Part 3 of the Digital Economy Act 2017. This requires the commercial providers of online pornography to have age verification arrangements in place to make sure users are aged 18 years or over. It has never been commenced.

6.4 Comment

Will Gardner, Director of the UK Safer Internet Centre at Childnet, said the Bill was a "significant step toward ensuring all children and young people

---

76 See, for example: Digital, Culture, Media and Sport Committee, The Draft Online Safety Bill and the legal but harmful debate (PDF), January 2022, p9; Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill (PDF), chapter 5

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

have a safe and enjoyable time online". He also said the inclusion of age verification for pornography was "important".[78]

Barnardo's Chief Executive, Lynn Perry, said she was "delighted" that all websites would be required to protect children from pornographic content. However, she wanted "action taken as soon as possible" by commercial pornography companies to introduce age verification to protect children.[79]

In contrast, Jim Killock, Executive Director of the Open Rights Group, has said the Government's proposals on pornography appeared to be "a huge boon to age verification companies, for little practical benefit for child safety, and much harm to people's privacy."[80]

78 Quoted in "The Online Safety Bill Has Been Introduced to Parliament", UK Safer Internet Centre blog, 17 March 2022 (accessed 25 March 2022)

79 "Online Safety Bill to be introduced to Parliament", Barnardo's news release [online], 17 March 2022 (accessed 25 March 2022); "Almost 70% of UK adults support tighter controls on online pornography content", Barnardo's news release [online], 31 March 2022 (accessed 31 March 2022)

80 "People to age verify before using Google or Reddit", Open Rights Group press release [online], 8 February 2022 (accessed 25 March 2022)

7 Protecting adults

As noted in the summary to this briefing, much harmful online content is not illegal but can have devastating effects. Such content can include material promoting self-harm and suicide, abusive language, bullying, and disinformation. Under the Bill, Category 1 services would have additional duties to protect adults from legal but harmful content.

7.1 What is content that is legal but harmful to adults?

The obligations of Category 1 services in relation to content that is "legal but harmful" have been controversial since the publication of the Online Harms White Paper. One of the concerns raised by commentators, organisations, and select committees, has been that platforms could "over-remove" legal content, affecting freedom of expression.[81]

In a Written Ministerial Statement of 17 March 2022 announcing the introduction of the Bill, Nadine Dorries, the Secretary of State for Digital, Culture, Media and Sport, said changes had been made to take account of these concerns:

> …We have refined the approach to defining content that is harmful to adults, so that all types of harmful content that category 1 services (the largest online platforms with the widest reach, including the most popular social media platforms) are required to address will be set out in regulations subject to approval by both Houses. This will provide clarity about the harms that services must address and will reduce the risk of category 1 services taking an overly broad approach to what is considered harmful…[82]

Clause 54(3) of the Bill categorises "content that is harmful to adults" as:

- priority content harmful to adults (**clause 54(3)(a**), or
- another type of content presenting "a material risk of significant harm to an appreciable number of adults in the UK" (**clause 54(3)(b)**).

Under **clause 54(2)**, the Secretary of State would specify in regulations when content would be priority content harmful to adults. The regulations would be subject to the draft affirmative procedure or, in urgent cases, made

81 For discussion, see the Library Paper, Regulating online harms (PDF) (15 March 2022)
82 DCMS, Online Safety, Written Ministerial Statement (HCWS691), 17 March 2022

affirmative procedure.[83] The Secretary of State would have to consult Ofcom before making any regulations (**clause 55(5)**).

7.2 Protecting adults from legal but harmful content

Clause 12 of the Bill would require an adults' risk assessment. This would require a provider to take account of, among other things:

- who uses the service.
- the level of risk that adults using the service may encounter each kind of priority content that is deemed harmful to adults (with each kind separately assessed), taking into account (in particular) algorithms used by the service, and how easily, quickly and widely content may be disseminated by the service.
- the level of risk of harm to adults presented by different kinds of priority content that is harmful to adults.
- the level of risk of harm to adults presented by priority content that is harmful to adults which particularly affects individuals with a certain characteristic or members of a certain group.
- the level of risk of functionalities of the service facilitating the presence or dissemination of priority content that is harmful to adults, identifying and assessing those functionalities that present higher levels of risk.
- the different ways in which the service is used, and the impact of such use on the level of risk of harm that might be suffered by adults.

Clause 13(2) would require a provider to summarise the findings of its latest adults' risk assessment in its terms of service.

Clause 13(3) would require a provider to state in its terms of service how it would treat each kind of priority content that is harmful to adults in a way described in **clause 13(4)**. The types of treatment listed in sub-clause (4) are:

- taking down the content.
- restricting users' access to the content.
- limiting the recommendation or promotion of the content.

[83] DCMS/Home Office, Delegated Powers Memorandum on the Online Safety Bill (PDF), p18

- recommending or promoting the content.

Clause 13(5) would require a provider to set out, in its terms of service, its response to the findings of its adults' risk assessment, referring to what the terms say about how each kind of priority harm is to be treated and any other provisions designed to mitigate or manage the identified risks. The terms of service would have to be clear and accessible, and applied consistently in relation to content that a provider reasonably considered to be priority content that was harmful to adults (**clause 13(6)**).

Clause 13(7) would require a service provider to notify Ofcom about the kinds and incidence of any non-designated harmful content to adults that it became aware of on its service.

User empowerment and user verification duties

On 25 February 2022, the Government announced that a "user verification duty" and a "user empowerment tools duty" had been added to the Bill.[84] This was in response to concerns raised by the Joint Committee on the draft Bill,[85] the DCMS Committee,[86] and the Petitions Committee[87] about the impact of abuse, including anonymous abuse, and the need to give users more control over who they interacted with.

The announcement of a "user verification duty" was welcomed by the Clean up the Internet organisation.[88] However, the Open Rights Group claimed that identity verification could lead to a "two tier internet".[89]

User empowerment duties

Under clauses 14(2) and (3) of the Bill, Category 1 services would need to have features in place to allow adult users to control what priority legal but harmful content they could see. These features would:

- reduce the likelihood of the user encountering "priority content that was harmful to adults", or particular kinds of such content, by means of the service; or

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

85 Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill (PDF), December 2021, pp32-5

86 Digital, Culture, Media and Sport Committee, The Draft Online Safety Bill and the legal but harmful debate (PDF), January 2022, pp10-4

87 Petitions Committee, Tackling Online Abuse (PDF), February 2022, chapter 6

88 Kinsella S, "Welcome announcement of a new "User Verification Duty"", Clean up the Internet blog post, 1 March 2022 (accessed 25 March 2022); Kinsella S, First thoughts on the revised Online Safety Bill, Clean Up the Internet blog post, 22 March 2002 (accessed 7 April 2022)

89 "The Online Safety Bill and Government crackdown on anonymity will punish victims", Open Rights Group press release [online], 25 February 2022 (accessed 25 March 2022)

- alert the user to the harmful nature of priority content that was harmful to adults that the user may encounter by means of the service.

Under **clauses 14(6) and (7)**, Category 1 services would need to have features in place to:

> (a) prevent non-verified users from interacting with content which that user generates, uploads or shares on the service; and
>
> (b) reduce the likelihood of that user encountering content which nonverified users generate, upload or share on the service.

User identity verification

Clause 57 would require Category 1 services to offer adult users the option to verify their identity. The verification process could be "of any kind" and would not require documentation to be provided. Providers of Category 1 services would need to make clear to users in their terms of service what form of identity verification was available and how the process would work.

Ofcom would publish guidance to help service providers comply with the user identity verification duty (**clause 58**).

7.3 Comment

Critics remain unconvinced about the Bill's provisions on adults and "legal but harmful" content.

The Carnegie UK Trust claims the Bill "remains weak on harms to adults" because the types of harms to be prioritised will not be set out until the Bill has received Royal Assent, and because the duty to protect adults from legal but harmful content would only apply to Category 1 providers.[90]

Robert Colvile, Director of the Centre for Policy Studies, has said the Bill makes "welcome steps towards restricting the scope of the 'legal but harmful' aspect of the Bill" and that a strengthened role for Parliament was a "necessary development". However, he remained "deeply concerned" that this aspect of the Bill could have "chilling effects on freedom of speech online", even with parliamentary oversight.[91]

Samaritans CEO, Julie Bentley, has claimed there is a "gaping hole that fails to protect adults from 'legal but harmful' suicide and self-harm content":

---

90 Perrin W et al, The Online Safety Bill: Our initial analysis (PDF), Carnegie UK Trust, 30 March 2022 (accessed 2 April 2022), p9

91 "Online Safety Bill still faces serious problems", Centre for Policy Studies press release [online], 17 March 2022 (accessed 25 March 2022)

> …All sites, not just the most popular, should at the very least carry out risk assessments of their suicide and self-harm content in relation to adults and make it clear how they will deal with harmful content. If nothing changes in the Bill then it will be a huge, missed opportunity to help prevent suicide.[92]

The Open Rights Group and Big Brother Watch have been long-standing critics of the Government's proposals to address online harms. According to the Open Rights Group, allowing Parliament to "rubber stamp" what ministers have decided to be "legal but harmful" means the "boundaries of online censorship will be politically driven, rather than defined by laws governed by human rights".[93] Big Brother Watch has said the Bill is a "censor's charter" that makes a "mockery of free speech".[94]

The Institute of Economic Affairs said the continued inclusion of "legal but harmful" content was a "recipe for disaster" because companies would take a cautious approach to anything that could potentially be unlawful, in order to avoid fines.[95]

Daniel Pryor, Head of Research at the Adam Smith Institute has claimed the Bill's provisions on legal but harmful speech are "wrong-headed".[96]

Other commentators, such as Laura Higson-Bliss, have argued the concept of harm needs to be given "a more precise meaning" to protect freedom expression.[97]

Paul Bernal, a lecturer in Information Technology and Media Law at the University of East Anglia, has claimed the Bill is a "grand gesture" that will "almost certainly do far more harm than good". According to Bernal, "smaller, piecemeal legislation dealing with particular harms" would be a more logical and effective way of dealing with problems encountered online.[98]

---

92 "Samaritans response to the Online Safety Bill", Samaritans news story [online], 17 March 2022 (accessed 25 March 2022)

93 Killock J, "Online safety made dangerous", Open Rights Group blog, 17 March 2022 (accessed 25 March 2022)

94 "Big Brother Watch responds to publication of the Online Safety Bill", Big Brother Watch press release [online], 17 March 2022; "The Telegraph – the Online Safety Bill makes a mockery of free speech", Big Brother Watch blog, 18 March 2022 (both accessed 25 March 2022)

95 "Online Safety Bill will seriously undermine free speech and privacy, warns IEA expert", IEA press release [online], 16 March 2022 (accessed 25 March 2022)

96 "The Online Safety Bill is an illiberal mess", Adam Smith Institute news [online], 17 March 2022 (accessed 25 March 2022)

97 Higson-Bliss L, "Online safety bill: ambiguous definitions of harm could threaten freedom of speech – instead of protecting it", The Conversation [online], 17 March 2022 (accessed 25 March 2022)

98 Bernal P, "Do we even need an Online Safety Bill?", Paul Bernal blog, 18 March 2022 (accessed 25 March 2022)

8 Protecting democratic and journalistic content

The Bill would place additional duties on Category 1 services in relation to "content of democratic importance" and "journalistic content".

8.1 Content of democratic importance

Clause 15(2) would require Category 1 services to use "proportionate systems and processes designed to ensure that the importance of the free expression of content of democratic importance is taken into account when making decisions about":

> (a) how to treat such content (especially decisions about whether to take it down or restrict users' access to it), and
>
> (b) whether to take action against a user generating, uploading or sharing such content

Clause 15(3) would require the systems and processes to be applied in the same way to a wide diversity of political opinion. The Explanatory Notes state this is "to ensure that Category 1 services do not privilege some political opinions over others when deciding how to protect content of democratic importance".[99]

There would also need to be provisions in the terms of service specifying the policies and processes designed to take account of the principle of clause 15(2), including how that principle would be applied to decisions (**clause 15(4)**). The provisions of the terms of service would have to be clear and accessible and applied consistently (**clause 15(5)**).

Clause 15(6) states that content is "content of democratic importance" in relation to a user-to-user service if:

> (a) the content is—
>
> (i) news publisher content in relation to that service, or
>
> (ii) regulated user-generated content in relation to that service; and

[99] Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, para 127

> (b) the content is or appears to be specifically intended to contribute to democratic political debate in the United Kingdom or a part or area of the United Kingdom.

"News publisher content" and "regulated user-generated content" are defined in **clause 49**.

8.2 Journalistic content

Since the Online Harms White Paper was published, there has been concern about what the Government's proposals could mean for journalistic content.[100] Content published on a newspaper or broadcaster's website is not in scope and user comments on that content is exempt. However, journalistic content on Category 1 services is in scope.

Clause 16(2) would require Category 1 services to operate a service "using proportionate systems and processes designed to ensure that the importance of the free expression of journalistic content is taken into account when making decisions about":

> (a) how to treat such content (especially decisions about whether to take it down or restrict users' access to it), and
>
> (b) whether to take action against a user generating, uploading or sharing such content.

Clause 16(8) defines "journalistic content" as "news publisher content" or "regulated user-generated content" that is generated for the purposes of journalism and which is "UK-linked" (as defined in **clause 16(9)**). The Explanatory Notes state that this includes, but is not limited to, "content generated by news publishers, freelance journalists and citizen journalists".[101]

There would be a duty, under **clause 16(3)**, to make a dedicated and expedited complaints procedure available to a person when content was taken down, or access to it restricted, and the person considered it to be journalistic content. The person would have to be:

- the user who generated, uploaded or shared the content on the service, or
- the creator of the content.

---

100 See, for example, House of Lords Communications and Digital Committee, Free for all? Freedom of expression in the digital age (PDF), July 2021, pp43-5 and pp106-9; Library Paper, Regulating online harms (PDF) (15 March 2022)

101 Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, para 132

Clauses 16(12) and (13) explain that "creator of content" means the "recognised news publisher" in question or:

- an individual who created the content and is in the UK; or
- an entity which created the content and is incorporated or formed under the law of any part of the UK.

Clause 50 defines "recognised news publisher". **Clause 50(1)** states that the BBC, Sianel Pedwar Cymru, and any entity that holds a licence under the Broadcasting Act 1990 or 1996, and which publishes news-related content under that licence, would qualify as a recognised news publisher.

Clauses 50(1)(d) and **50(2)** set out when an entity would also be a recognised news publisher.

An entity could not be a recognised news publisher if it met the criteria but was a proscribed organisation under the Terrorism Act 2000 or was an entity that supported such an organisation (**clause 50(3)**).

Under **clause 16(4)**, Category 1 providers would have to make a dedicated and expedited complaints procedure available to users in relation to a decision to act against a user because of content generated, uploaded or shared by the user and which the user considered to be journalistic content.

The Secretary of State has said that the Bill's provisions would help to "recognise and defend the invaluable role of a free press". Moreover, as the Bill progressed, she had "every intention of further improving the requirements for platforms not to remove content from recognised media outlets".[102]

8.3 Comment

The Society of Editors has welcomed the Government's assurances that it plans to strengthen protections for journalists and freedom of expression during the Bill's stages. Executive Director, Dawn Alford, commented:

> …the bill does not, in its present form, do enough to protect legitimate journalistic content and further amendments must be added as a matter of priority if the government is to fulfil its manifesto pledge of defending freedom of expression.

[102] Dorries N, "How we will narrow the ground for barring harmful posts in the Online Safety Bill", Conservative Home website, 15 March 2022 (accessed 25 March 2022)

> What we now need to see is additional safeguards to protect journalistic content from take-down by broad-brush algorithms and it is essential that any appeals process reflects the fast-paced nature of news…[103]

The Open Rights Group has been more critical, claiming the Bill could lead to "backdoor press regulation":

> Because there are exemptions to allow the press to say vile but lawful things which the rest of us cannot, Ofcom must determine who the press are. In practice this will mean that, for instance, a publisher can show they are a member of a press body, such as a regulator. Thereby the state will now regulate who is allowed to be the media, at least in order to avoid online censorship. The press do not seem to have realised that they have conceded something they have campaigned against for decades.[104]

103 "Society welcomes commitment to strengthening journalistic protections during Online Safety Bill passage", Society of Editors news [online], 17 March 2022 (accessed 25 March 2022)

104 Killock J, "Online safety made dangerous", Open Rights Group blog, 17 March 2022 (accessed 25 March 2022)

9 Duties about fraudulent advertising

The Government has added a new legal duty to the Bill (**clauses 34**, **35** and **36**). This would require large social media platforms (defined in the Bill as Category 1 services) and search engines (defined as Category 2A services) to take steps to prevent fraudulent paid-for adverts appearing on their services.

When first published in May 2021, the draft Bill only covered user-generated content. This amended version of the Bill brings paid-for adverts in scope, whether controlled by the platform itself or an advertising intermediary. The aim is to protect internet users from the potentially devasting impact of fraudulent adverts.[105]

Separately, on 9 March 2022, the Government launched a public consultation on its Online Advertising Programme. This is a review of the regulatory framework of paid-for online advertising to tackle the lack of transparency and accountability across the whole supply chain. The aim is to bring more of the major players under regulation. This review will work in conjunction with the measures being introduced in the Online Safety Bill.

There is a separate Library briefing on Consumer protection: online scams.[106] In addition to looking at the scale of the problem, it considers the different types of scams, and who are the targeted victims.

9.1 Background

Online advertising

Online advertising dominates advertising globally. According to the DCMS, global investment in ad spend is predicted to be in the region of $700 billion by the end of 2022, with digital advertising contributing to around half of that figure.[107] The Office for National Statistics (ONS) estimates the total

105 Department for Digital, Culture, Media & Sport press release, Major law changes to protect people from scam adverts online, 8 March 2022

106 Consumer protection: online scams, Commons Library briefing, CBP-9214

107 Department for Digital, Culture, Media & Sport press release, Major law changes to protect people from scam adverts online, 8 March 2022, see also WARC, Global Ad Trends: Ad Investment 2021/22

turnover of the UK advertising industry in 2019 as £40 billion; it generated £17 billion in Gross Value Added (GVA) and exported £4 billion in services.[108]

Ofcom has stated that with the growth in internet consumption, "advertising has become the primary source of revenue for many online businesses" and underpins the provision of key online services such as search and social media.[109]

Current regulation of paid-for advertising

In the UK, paid-for online advertising is regulated through the UK Code of Non-Broadcast Advertising and Direct & Promotional Marketing (known as the CAP Code) and consumer protection legislation. Compliance with the CAP Code is overseen by the Advertising Standards Authority (ASA), who holds advertisers primarily responsible for the creative content, media placement and audience targeting of their online ads. The ASA also places responsibilities on others involved in preparing or publishing marketing communications (such as agencies, publishers, and other service suppliers) to comply with the CAP Code.

There is a separate Library briefing on the Regulation of advertising by the ASA.[110] The ASA has also published guidance, Innovate to regulate- policing ads online.[111]

A criticism of the current self-regulation approach to online advertising is that the ASA has relatively restricted powers based around 'naming and shaming' and banning offending ads.[112] In broadcast advertising, licences can be revoked where there are serious breaches, but there are no equivalent sanctions for those that host harmful content online. A further criticism is that whilst parties involved in preparing or publishing ads have a role to play in ensuring the ads are honest and responsible, "there are limited circumstances in which online service providers are held by the ASA to exercise primary control over the creative content and audience targeting of adverts".[113]

Platforms and intermediaries have their own governing principles, terms of service and community guidelines. They do have certain obligations under consumer law, for example, a duty to trade fairly under the Consumer Protection from Unfair Trading Regulations 2008. However, as highlighted by the DCMS, "there are often limited obligations on them to share information

108 Department for Digital, Culture, Media & Sport press release, Major law changes to protect people from scam adverts online, 8 March 2022, see also Office for National Statistics, Non-financial business economy: sections A to S, 21 June 2021

109 Ofcom, Online Nation report, 30 May 2019

110 Regulation of advertising by the ASA, Commons Library briefing, CBP-6130

111 Innovate to regulate- policing ads online, Advertising Standards Authority [online], 8 July 2021 (accessed 22 March 2022)

112 Department for Digital, Culture, Media & Sport, Online Advertising Programme Consultation, 9 March 2022

113 Ibid

relating to monitoring, performance and propriety",[114] with no standardised practice across industry.

A further concern for the DCMS is that many larger platforms offer 'self-service' advertising buying services, where there is little vetting for advertisers:

> As a result, bad actors often operate with relative impunity, using online advertising as a means to perpetrate fraud or advertise other illegal or legal but harmful products and services, with limited oversight.[115]

The DCMS wants 'transparency' and 'accountability' spread across the supply chain, so that intermediaries, platforms, and publishers play a greater role in the regulation of online paid for advertising.[116]

Joint Committee's recommendation

Paid-for adverts were not included in the original draft Online Safety Bill; it only covered user-generated content on user-to user services and search services. It was the Government's view that including paid-for adverts would not work and would extend the scope of the Bill in a way that would not be appropriate.[117] Instead, paid-for advertising and scams were to be considered as part of the DCMS's Online Advertising Programme (see below).

During its pre-legislative scrutiny of the draft Bill, the Joint Committee heard evidence that this exclusion would create a gateway for various harms to spread online.[118] For example, the Financial Conduct Authority (FCA) told the Joint Committee that: "the problem [of online fraud] is most manifest in the paid-for space, so it does not make sense for the Bill not to deal with the very heart of the problem, which is the paid-for advertising space".[119] The consumer group Which? explained that "paid-for advertising on online platforms is a primary method used by criminals to target consumers and engage them in a [financial] scam, as it gives them instant access to large numbers of target audiences".[120] Other witnesses suggested that if paid-for advertising remained excluded from scope, criminals might switch to paying for fraudulent content to be disseminated.[121] The ASA confirmed that

114 Ibid
115 Ibid
116 Ibid
117 House of Commons, Joint Committee on the Draft Online Safety Bill, Report HC 609 of session 2021-22, 10 December 2021
118 Ibid
119 Ibid, Q 121
120 Ibid, Written evidence from Which? (OSB0115)
121 Ibid, this concern is raised in written evidence from: Reset (OSB0138) and Dame Margaret Hodge MP (OSB0201), and oral evidence by the FCA (Q 120), Which? (Q 112), Martin Lewis (Q 112), and Ofcom (Q 263).

research showed "increasing concerns about scams are influencing the public's trust in online ads."[122]

In its report, published in December 2021, the Joint Committee recommended significant changes to the draft Bill, including bringing paid-for advertising within scope of the Bill to tackle scams and fraud.[123] In making this recommendation, the Joint Committee said:

> The exclusion of paid-for advertising from the scope of the Online Safety Bill would obstruct the Government's stated aim of tackling online fraud and activity that creates a risk of harm more generally. Excluding paid-for advertising will leave service providers with little incentive to remove harmful adverts, and risks encouraging further proliferation of such content.[124]

The Joint Committee also suggested that Ofcom should be responsible for acting against service providers who consistently allow paid-for advertisements that create a risk of harm to be placed on their platform:

> We recommend that the Bill make clear Ofcom's role will be to enforce the safety duties of providers covered by the online safety regulation, not regulate the day-to-day content of adverts or the actions of advertisers. That is the role of the Advertising Standards Authority. The Bill should set out this division of regulatory responsibility.[125]

The Government published its response to the Joint Committee's report on 17 March 2022.[126] It said it would bring paid-for advertising within scope of the Bill by "introducing a new standalone duty to require the highest risk and highest reach platforms (including large search services) to minimise the likelihood of fraudulent adverts being published on their service and protect their users".[127] In tandem with its response, the Government published the amended Bill for introduction.

Online Advertising Programme consultation

The Online Safety Bill is intended to work in conjunction with the Government's Online Advertising Programme as well as other measures it is developing to address competition and data protection issues online.

In 2019, the DCMS announced that it would consider how online advertising is regulated in the UK. In 2020, it ran a call for evidence[128] focusing on online content and placement standards.

---

122 Ibid, Q 118

123 Ibid

124 Ibid, para. 268-271

125 Ibid

126 Department for Digital, Culture, Media & Sport, Joint Committee report on the draft Online Safety Bill: Government response, Cm 640, 17 March 2022

127 Ibid

128 Department for Digital, Culture, Media & Sport, Online advertising – call for evidence, 27 January 2020

A public consultation on the Government's Online Advertising Programme was published on 9 March 2022, as part of a wider overhaul of how online advertising is regulated in the UK, including proposals to improve transparency and accountability and tackle harmful, fraudulent and misleading adverts.[129] The DCMS is currently seeking views on three options for regulatory reform:

- Self-regulatory approach. This would be centred around the ASA's existing regulatory role in enforcing the CAP Code and the proposed ASA 'Online Platforms and Network Standards' (OPNS), which is being developed. The aim being to increase accountability and transparency across the supply chain.

- A statutory backstop approach. The ASA would continue as the frontline regulator but would be supported by a newly appointed statutory regulator, to provide stronger powers of enforcement where needed.

- Full statutory approach. This would involve appointing a statutory regulator to introduce measures designed to increase transparency and accountability and issue Codes of Practice. This regulator would be responsible for regulation and enforcement, with a range of powers.

Explaining the overriding aim of this Online Advertising Programme (OAP) consultation, the Government said:

> The OAP … [is] seeking to provide a holistic review of the whole ecosystem for online advertising, examining the role of actors across the supply chain and creating a transparent and accountable market. We will continually examine the interdependencies and overlaps between this review and other regulatory initiatives across government and industry to ensure consistency and coherence in our approach, in line with the government's Plan for Digital Regulation[130] published in July 2021.[131]

Some issues are outside the scope of the consultation including privacy issues,[132] data policy, political advertising, competition issues,[133] and user generated content (except where it is also paid-for content covered by the Online Safety Bill).

The consultation closes on **1 June 2022**. The Government has said it intends to respond to the consultation and outline proposals to reform online advertising later this year.

---

129 Department for Digital, Culture, Media & Sport, Online Advertising Programme Consultation, 9 March 2022

130 Department for Digital, Culture, Media & Sport, Digital Regulation: Driving growth and unlocking innovation, 6 July 2021 (updated 9 March 2022)

131 Department for Digital, Culture, Media & Sport, Online Advertising Programme Consultation, 9 March 2022

132 Since 2019, the Information Commissioner's Office has been looking separately at the use of adtech in targeting adverts to consumers through programmatic advertising

133 Dealt with by the new pro-competition regime for digital markets

9.2 The fraudulent advertising duty

A new duty has been added to the Online Safety Bill requiring large social media platforms and search engines to prevent paid-for fraudulent adverts appearing on their services (whether they are controlled by the platform itself or an advertising intermediary).[134]

Specifically, under **clauses 34(1)** large social media platforms (defined in the Bill as Category 1 services) would be required to operate their services using proportionate systems and processes designed **to:**

- prevent (or minimise in the case of search engines) individuals from encountering fraudulent advertising,
- minimise the amount of time that fraudulent advertising is present, and
- swiftly remove fraudulent advertising once they are made aware of it through any means. (i.e., takedown requirements).

Clause 35 would impose a similar duty on search engines (defined as Category 2A services) to operate the service using proportionate systems and processes designed to minimise (rather than prevent) the risk of individuals encountering content consisting of fraudulent advertisements in or via search results of the service.

The Bill considers what is meant by references to "encountering" fraudulent advertisements in or via search results using a search engine (**clause 35(4)**). This includes interacting with a paid-for advertisement in search results (e.g., by clicking on the fraudulent ad in a search result and then being redirected to a web page). "Encountering" does not include any subsequent interactions with a website (e.g., leaving the original fraudulent advertisement web page).

In determining what is 'proportionate' regarding social media platforms and search engine's systems and processes, the following factors are relevant:

- the nature, and severity, of potential harm to individuals presented by different kinds of fraudulent advertisement, and
- the degree of control a provider has in relation to the placement of advertisements on the service.

This recognises that large social media platforms (**clause 34(5)**) and search engines (**clause 35(6)**) may rely on third party intermediaries to display paid

[134] Department for Digital, Culture, Media & Sport press release, Major law changes to protect people from scam adverts online, 8 March 2022

advertisements on its service and will, therefore, have less control over measures to prevent posting of fraudulent adverts.

Importantly, social media platforms and search engines must also include clear and accessible information in their terms of service (or in a publicly available statement in the case of search engines) about any proactive technology that it will use to comply with its duties in respect of fraudulent advertising (**clauses 34(2)** and **35(2)**).

An advertisement appearing on a large social media platform or search engine is "fraudulent" if:

- it is a paid-for advertisement,[135]
- it amounts to an offence specified in section 36,[136]
- and (in relation to social media platforms only) it is not regulated user-generated content in relation to the service.[137]

The Bill contains a list of offences that will constitute fraud offences in relation to duties about fraudulent advertising (**clause 36**). The relevant inchoate offences also apply to the definition of fraud offences (i.e., attempting or conspiring to commit an offence).

According to the DCMS, if enacted, this new legal duty will mean companies operating social media platforms and search engines must "clamp down on ads with unlicensed financial promotions, fraudsters impersonating legitimate businesses and ads for fake companies".[138]

The detail of what platforms and search engines will need to do to fulfil their new duty will be set out in Ofcom Codes of Practice. The Government has said that this could include making firms scan for scam adverts before they are uploaded to their systems, using identity verification, and checking financial promotions are made only for FCA-authorised firms.[139] Ofcom will oversee whether companies have adequate measures in place to fulfil the duty, but will not assess individual pieces of content, in keeping with the approach taken in the rest of the Bill. Ofcom will have the power to hold companies to account by blocking their services in the UK or issuing heavy fines of up to £18 million or ten per cent of annual turnover.[140]

135 See clause 189

136 Construed in accordance with clause 52(3) and (9) (for social media platforms), and construed in accordance with clause 52(3) and (9) (for search engines)

137 See clause 49

138 Ibid

139 Department for Digital, Culture, Media & Sport press release, Major law changes to protect people from scam adverts online, 8 March 2022

140 Ibid

9.3 Comment

Martin Lewis, founder of MoneySavingExpert.com and the Money and Mental Health Policy Institute, who gave evidence to the Joint Committee during its pre-legislative scrutiny of the draft Bill, said:

> The Government is now accepting the principle that scam adverts need to be included, and that firms who are paid to publish adverts need to be responsible for them, is a crucial first step. Until now, only user-generated scams were covered – which risked pushing more scam ads, incentivising criminals to shift strategy. Yet it is a complex area. Now we and others need to analyse all elements of this new part of the Bill, and work with Government and Parliament to close down the hiding places or gaps scammers can exploit.[141]

On publication of the Bill, the Financial Conduct Authority (FCA) said:

> We welcome that the Online Safety Bill will now require the largest platforms to tackle fraudulent advertising. We have been clear about the need for legislation and appreciate the Government's positive engagement on this.[142]

The consumer body Which? has also campaigned for the inclusion of scam ads in the Online Safety Bill. Commenting on the Government's decision to extend the scope of the Bill, it said:

> This could make a huge difference to stemming the tide of fake and fraudulent ads on social media and search engines which cause devastating financial and emotional harm to innocent victims. The Online Safety Bill must now ensure that the regulator has the support and resources it needs to hold companies to account and take strong enforcement action where necessary, so that fraudsters are prevented from using adverts to lure unsuspecting victims.[143]

The ABI (Association of British Insurers) has also welcomed the changes to the Online Safety Bill:

> [We] are pleased the Government has listened to the many different sectors and organisations, including our own, which have called for paid-for fraudulent adverts to be stopped on social media platforms and search engines. It's essential this happens to prevent vulnerable customers being scammed and to ensure the Bill meets its central objective of making the UK the "safest place in the world to be online". We will analyse this complex Bill when it is introduced into Parliament to ensure that no gaps are left for scammers to exploit, and that Ofcom is given the necessary enforcement powers to punish those that break the law.[144]

---

141 Ibid

142 Ibid

143 Ibid, see also Government must include scam ads in the Online Safety Bill, Which? [online], 25 February 2022, (accessed 22 March 2022)

144 ABI welcomes changes to Online Safety Bill, Association of British Insurers (ABI), 9 March 2022, (accessed 22 March 2022)

However, the Advertising Association (a body that represents UK advertisers, agencies, media owners and tech companies) said the Bill would have significant implications for all relevant stakeholders:

> Whilst bad actors indeed need to be dealt with through appropriate enforcement, the Online Safety Bill now seems to be widening its scope on the same day as the Online Advertising Programme is published, promising a comprehensive review of online advertising and the way it is regulated. This legislation will have significant implications for all relevant stakeholders and needs to be considered very carefully.
>
> […]
>
> Advertising and its online ecosystem is an essential engine for our country's GDP, providing a lifeline for businesses, large and small, to carry on serving customers, even during the toughest of lockdown conditions.
>
> We are proud too that the UK has a gold-standard self-regulatory system encompassing the CAP Code, IAB Gold Standard, TAG, Global Alliance for Responsible Media, the Financial Audit Toolkit and robust industry standards and deliver a multi-faceted framework to regulate online advertising. New initiatives will further enhance this framework including ISBA's Origin trial and TAG Trustnet. It is vital any future regulation considered during this consultation is proportionate and complements the existing framework.[145]

[145] AA Statement: Online Safety Bill and Online Advertising Programme, Advertising Association [online], 9 March 2022, (accessed 22 March 2022)

10 Ofcom's powers and duties

Part 7 sets out Ofcom's duties and powers as the online safety regulator. Ofcom's costs would be met through fees charged to in scope service providers. Under **part 6** of the Bill, these would be charged to providers whose "qualifying worldwide revenue" was equal to or greater than a "threshold figure" (as set by the Secretary of State, after taking advice from Ofcom).

10.1 General duties

Clause 77 would amend the Communications Act 2003 to give Ofcom a general duty to secure "the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm."

Clause 78 sets out Ofcom's duties in relation to statements of strategic priorities designated by the Secretary of State under **clause 143(1)**.

Clause 79 would require Ofcom to carry out impact assessments on proposals to introduce, replace or amend codes of practice under the Bill. These would have to include an assessment of the likely impact on small and micro businesses.

Ofcom's further duties are briefly summarised below. The Explanatory Notes to the Bill provide further detail.[146]

Register of regulated services

Chapter 2 would require Ofcom to establish, publish and maintain a register of each regulated service that met the threshold conditions set out in **Schedule 10** and would therefore be designated as a Category 1, 2A or 2B service.

[146] Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, pp65-91

Risk assessments

Chapter 3 would require Ofcom to carry out risk assessments to identify and assess the risks of harm to individuals presented by in scope services. The assessments would cover:

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

A register of the risks of services would then have to be published.

10.2 Information gathering and sharing

Chapter 4 would give Ofcom the power to issue information notices to obtain any information it needed to carry out its online safety functions. These could be issued to individuals at: providers of a user-to-user service, a search service, an internet service providing pornography, an "ancillary service", an "access facility", and any other person who Ofcom thought able to provide relevant information (**clause 85**).

Ofcom would have the power to require, in an information notice, that a "senior manager" was named who would be responsible for ensuring compliance with the notice (**clause 87**). The draft Bill would have deferred this power for two years. However, in a press release announcing publication of the Bill, the Secretary of State explained that the period would be reduced "to two months to strengthen penalties for wrongdoing from the outset".[147] Under **clause 93**, senior managers would be criminally liable for failing to prevent an information offence. Prosecution would only happen where a regulated provider had already been found liable for failing to comply with Ofcom's information request. The offence would have extra-territorial application (under **clause 167(2)**).

Clauses 88 and 89 set out when Ofcom would be able to open an investigation and conduct interviews where a service provider had failed or was failing to comply with a relevant requirement.

Clause 91 and Schedule 11 set out Ofcom's powers of entry, inspection and audit.

Clause 97 would give Ofcom the power to collaborate and share information with an overseas regulator to help that regulator exercise their online safety

147 "World-first online safety laws introduced in Parliament", DCMS press release [online], 17 March 2022 (accessed 22 March 2022)

functions, or to cooperate with any related criminal investigations or proceedings. The power would only apply in relation to an overseas regulator specified in regulations made by the Secretary of State.

The Carnegie UK Trust thinks it "curious" that clause 97 makes express provision for Ofcom to work with overseas regulators, but not UK ones. According to the Trust, "it would do no harm to set out in the Bill a requirement on Ofcom to define the terms of its relationships with other regulators and the power, if needed, to get them to work effectively together".[148]

Information offences and penalties

The Bill includes various information offences. **Clause 92** would make it an offence for a person to:

- fail to comply with an information request.
- provide false information in response an information request.
- provide encrypted information, that it is not possible to understand, in response to an information request.
- suppress, destroy or alter information requested by Ofcom.

Clause 95 would make it an offence for a person to:

- intentionally obstruct or delay a person copying a document.
- fail to attend or participate in an interview with Ofcom.
- knowingly or recklessly provide false information when being interviewed by Ofcom.

Clause 94 sets out offences in connection with notices under **Schedule 11**.

Clause 96 would set the penalties for information offences.

The information offences in **clauses 92 and 95** would have extra-territorial application (under **clause 167(1)**).

[148] Perrin W et al, The Online Safety Bill: Our initial analysis (PDF), Carnegie UK Trust, 30 March 2022 (accessed 2 April 2022), p14

10.3 Notices to deal with terrorism content or CSEA content

Chapter 4 would give Ofcom the power to require a service provider to use accredited technology to identify and remove terrorism content on public channels and CSEA content on private and public channels. In giving a notice, Ofcom would have to take into account factors such as:

- the functionalities of the service.
- the service's user base.
- the prevalence of relevant content on a user-to-user service and the extent of its dissemination by means of the service.
- the level of risk of harm to individuals and the severity of that harm.
- the systems and processes used by the service to identify and remove relevant content.
- the extent to which the use of the specified technology would, or might result in, interference with users' right to freedom of expression (**clause 104(2)**).

Ofcom could impose a penalty on a service provider for failing to comply with a notice (**clause 119**).

10.4 Ofcom's enforcement powers

Chapter 6 sets out Ofcom's enforcement powers. Ofcom would be required to publish guidance on the use of these powers (**clause 129**).

Provisional notices and confirmation decisions

Under **clause 110**, Ofcom could issue a "provisional notice of contravention" when it had reached a provisional decision that an in-scope service had breached its duties. This would have to set out suggested requirements to comply with the duty or remedy breach and/or the financial penalties that Ofcom intended to impose.

If Ofcom's final decision was that a service had breached an enforceable requirement, a "confirmation decision" would be issued (**clause 112**). This would set out whether Ofcom required any specific steps to be taken and/or pay a financial penalty (under **clause 117**).

Ofcom could issue confirmation decisions relating to a providers' failure to:

- carry out an illegal content or children's risk assessment properly or at all; and identified a risk of serious harm that the regulated provider was not effectively mitigating or managing (**clause 114**).

- properly carry out a children's access assessment (**clause 115**).

Clause 116 sets out when a confirmation decision could require the use of "proactive technology".

A financial penalty could be imposed where there was a failure to complete the steps required in a confirmation decision (**clause 118**).

Financial penalties

Clause 122 and Schedule 12 set out details of the financial penalties that Ofcom would be able to impose on the providers of regulated services.

Under **Schedule 12(4)**, the maximum penalty would be £18 million or 10% of "qualifying worldwide revenue" (as defined in **paras 4(4)-(6) of Schedule 12**), whichever was greater.

Business disruption measures

Ofcom would be able to apply to the courts for "business disruption measures"- court orders requiring third parties to withdraw services or block access to non-compliant regulated services. They would be used for the "most serious instances of user harm".[149]

Service restriction orders (**clause 123**) would require the providers of "ancillary services" to take steps to disrupt the business or revenue of a non-compliant provider's operations. Ancillary services would include companies providing payment or advertising services.

Ofcom would also be able to apply for "interim restriction orders" (**clause 124**) where it was "likely" that a provider was failing to comply with its duties and the risk and severity of harm to users would mean that it was not appropriate to wait to establish the failure before applying for an order.

Access restriction orders (**clause 125)** would require internet services providers and app stores (for example) to take steps to prevent, restrict, or deter UK users from accessing a non-compliant service.

Interim restriction orders (**clause 126)** could be made where, for example, there was "serious user harm that requires quick action to impede access".[150]

149 Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, para 573
150 Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, para 579

10.5 Committees, research and reports

Clause 130 would require Ofcom to set up an advisory committee on disinformation and misinformation. The Explanatory Notes state this is "because the spread of inaccurate information, regardless of intent, is particularly concerning".[151] The Committee would provide advice to Ofcom on:

- how the providers of regulated services should deal with disinformation and misinformation.
- how Ofcom should exercise its power under clause 64 (on transparency reporting) relating to disinformation and misinformation.
- how Ofcom should exercise its duty to promote media literacy in relation to countering disinformation and misinformation on regulated services.[152]

Chapter 7 of Part 7 would also:

- require Ofcom to arrange research into users' opinions and experiences relating to regulated services (**clause 132**).
- amend section 16 of the Communications Act 2003 so that the Communications Panel could give advice on matters relating to different types of online content under the Bill (**clause 133**).
- require Ofcom to publish annual reports on the steps it had taken, when carrying out its online safety functions, to uphold users' rights under Articles 8 and 10 of the European Convention on Human Rights, as required by section 6 of the Human Rights Act 1998 (**clause 134**).
- require Ofcom to produce transparency reports, at least once a year, based on information from service providers' own transparency reports (**clause 135**).
- require Ofcom to publish a report about researchers' access to information from providers of regulated services **(clause 136)**.
- enable Ofcom to publish reports on online safety matters (**clause 137**).

151 Explanatory Notes to the Online Safety Bill (PDF), 17 March 2022, para 586

152 The duty to promote media literacy is set out in section 11 of the Communications Act 2003 (as amended)

11 Communications offences

Part 10 of the Bill would set out three new offences involving harmful, false or threatening communications, and a new offence of sending a photograph or film of a person's genitals to another person (commonly known as 'cyberflashing').

The new offences are based on recommendations made by the Law Commission following a review of the law on abusive and offensive online communications.

11.1 The current law on online offences

The Crown Prosecution Service website provides an overview of the current approach to prosecuting offensive online communications.

A range of criminal offences can cover offensive online communications including sexual offences, public order offences, stalking and harassment.

There are also specific communications offences under s127 of the Communications Act 2003 and s1 of the Malicious Communications Act 1988.

Under section 127 of the Communications Act 2003 a person commits an offence if they:

- send (or cause to be sent) by means of a public electronic communications network a message (or other matter) that is grossly offensive or of an indecent, obscene or menacing character; or
- send (or cause to be sent) by means of a public electronic communications network a message that the person knows to be false, or persistently make use of a public electronic communications network, in either case for the purpose of causing annoyance, inconvenience or needless anxiety to another

Under section 1 of the Malicious Communications Act 1988, it is an offence for a person to send to another person:

- a letter, electronic communication or article of any description which conveys a message which is indecent or grossly offensive, a threat, or information which is false and known or believed to be false by the sender, or

- any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature.

The section 1 offence is only committed if the purpose (or one of the purposes) of the sender in sending the communication was to cause distress or anxiety to the recipient or to any other person to whom the sender intends that it or its contents or nature should be communicated.

In recent years concerns have been raised that these communications offences – which predate the widespread use of social media platforms – are inadequate to deal with online harassment and abuse. There have therefore been calls for the Government to review the current law to ensure it is fit for purpose.[153]

11.2 The Law Commission review

In February 2018 Theresa May's Government asked the Law Commission to "review the laws around offensive communications and assess whether they provide the right protection to victims online".[154] The Reform of the Communications Offences project page on the Law Commission's website sets out full details of the project.

In November 2018 the Law Commission published a Scoping Report on Abusive and Offensive Online Communications. The report analysed the current state of the relevant criminal law and concluded that "in most cases abusive online communications are, at least theoretically, criminalised to the same or even a greater degree than equivalent offline behaviour".[155]

However, the Law Commission considered that there was nevertheless "considerable scope to improve the criminal law in this area" and that using the criminal law to deal with harmful online conduct was hindered by the following "practical and cultural barriers":

- the scale of abusive and offensive communications, and limited law enforcement capacity to pursue these
- a "persistent cultural tolerance" of online abuse, meaning it is not always treated as seriously as offline conduct

153 See for example the House of Commons Home Affairs Committee, Hate crime: abuse, hate and extremism online (PDF), Fourteenth Report of Session 2016–17, HC 609, 1 May 2017, para 56

154 Prime Minister's Office, PM speech on standards in public life, 6 February 2018. See also Law Commission press release, Government asks Law Commission to look at trolling laws, 6 February 2018

155 Law Commission, Abusive and Offensive Online Communications: A Scoping Report (PDF), Law Com No 381, November 2018, para 13.7

- difficulties in striking a balance between protecting people from harm and maintaining human rights to freedom of expression
- technical and financial barriers to pursuing online offenders
- jurisdictional and enforcement barriers to prosecution, given the "highly globalised" nature of the online environment.[156]

In June 2019 the Government announced that it had engaged the Law Commission to embark on the next phase of the review.[157]

The Law Commission launched a full consultation paper on 11 September 2020.[158] It identified the following issues with the existing communications offences in section 127 of the 2003 Act and section 1 of the 1988 Act:

- Vague and uncertain terminology, in particular phrases such as "grossly offensive" and "indecent", which could be in tension with the right to freedom of expression under Article 10 of the European Convention on Human Rights. The consultation paper noted that interferences with Article 10 rights are required to be "clearly prescribed by law".[159]
- Over-criminalisation of conduct that should not be criminal. The Law Commission said that one particular risk is the difficulty in determining when a communication crosses the threshold "from mere offensiveness to gross offensiveness". The offences also capture behaviour that is offensive but does not necessarily cause harm or pose a risk of harm.[160]
- Under-criminalisation of conduct that should be criminal. Some types of harmful conduct, such as 'pile-on harassment' or the encouragement of self-harm, may not be covered by the existing offences. Other harmful conduct may not be covered due to the technology used. For example, the s127 offence does not cover messages sent via a private network (e.g. Bluetooth or a local intranet).[161]
- Unsatisfactory targeting and labelling, which limits the scope of the offences to certain methods of delivery and fails to appropriately label or target harmful behaviour.[162]

156 Ibid, para 13.12
157 HCWS1659 Law Commission Review Update
158 Law Commission, Harmful Online Communications: The Criminal Offences – A Consultation paper (PDF), Consultation Paper 248 and Harmful Online Communications: The Criminal Offences – Summary of the Consultation Paper (PDF), September 2020
159 Law Commission, Harmful Online Communications: The Criminal Offences – A Consultation paper (PDF), Consultation Paper 248, paras 3.113-3.124
160 Ibid, paras 3.125-3.139
161 Ibid, paras 3.140-3.158
162 Ibid, paras 3.159-3.169

- Overlapping offences that "sit together somewhat awkwardly, and overlap in ways that cannot readily be explained".[163]

To address these issues, the Law Commission therefore sought views on a proposed new 'harm-based' communications offence and a range of other proposals.

The Law Commission published its final report and recommendations on 21 July 2021.[164] The final recommendations reflected a range of consultation feedback on issues such as freedom of speech, the definition of 'harm', and the intent of the sender.[165]

A summary of the final recommendations is set out on the Law Commission's website:

> In the report, we recommend the following new or reformed criminal offences:
>
> 1. **a new "harm-based" communications offence** to replace the offences within section 127(1) of the Communications Act 2003 ("CA 2003") and the Malicious Communications Act 1988 ("MCA 1988");
>
> 2. a new offence of encouraging or assisting serious self-harm;
>
> 3. a new offence of cyberflashing; and,
>
> 4. new offences of sending knowingly false communications, threatening communications, and making hoax calls to the emergency services, to replace section 127(2) of the CA 2003.
>
> Central to our recommended harm-based offence is a move away from a focus on broad categories of wrongful content (such as "grossly offensive"), to a more context-specific analysis: given those who are likely to see a communication, was harm likely? The aim is to ensure that communications that are genuinely harmful do not escape criminal sanction merely because they do not fit within one of the proscribed categories. Secondly, communications that lack the potential for harm are not criminalised merely because they might be described as grossly offensive or indecent, etc.[166]

The Law Commission also recommended the introduction of a specific offence to cover flashing images being sent maliciously to known sufferers of epilepsy, but did not make any recommendations as to the precise form of such an offence.

In its interim response to the Law Commission, the Government said it would legislate (by way of the Bill) to introduce the recommended harm-based

---

163 Ibid, paras 3.170-3.172

164 Law Commission, Modernising Communications Offences: A final report (PDF), Law Com No 399 and Modernising Communications Offences: Summary of the Final Report (PDF), July 2021

165 A high level overview of some of the concerns raised by consultees is set out in the House of Lords Communications and Digital Committee report Free for all? Freedom of expression in the digital age, HL Paper 54, 22 July 2021, paragraphs 99-111

166 Law Commission website, Reform of the Communications Offences [accessed 31 March 2022]

communications offence, the false communications offence and the threatening communications offence.[167] The Government subsequently confirmed that the cyber-flashing offence would also be included in the Bill.[168]

The Government has said it will continue to assess the remaining proposals – a hoax calls offence, an offence of encouraging or assisting serious self-harm, and an epilepsy-related flashing images offence – ahead of issuing a fuller response in due course.[169] These proposals are not included in the Bill.

11.3 Contents of the Bill

Part 10 of the Bill would introduce three new communications offences covering harmful, false or threatening communications, and a new 'cyberflashing' offence. Detailed clause by clause analysis is set out in paragraphs 628 to 656 of the Explanatory Notes (PDF).

Harmful, false or threatening communications

Clauses 150 to 155 of the Bill would introduce three new communications offences to replace the existing offences in subsections 127(1), (2)(a) and (2)(b) of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988.

The new offences would extend to England and Wales, although the Government has indicated that it will "extend the offences at clauses 150 and 151 to Scotland and Northern Ireland via government amendment, and will seek legislative consent from Scotland to do so".[170]

Clause 150 sets out the harmful communications offence, which would be committed if a person sends a message and at the time of sending the message:

- there was a "real and substantial risk that it would cause harm to a likely audience", with harm defined as "psychological harm amounting to at least serious distress"
- the person intended to cause harm to a likely audience

167 Department for Digital, Culture, Media and Sport, Letter to Professor Penney Lewis: The Government's Interim Response to the Law Commission's 'Modernising Communications Offences' report, 4 February 2022. See also DCMS/Home Office press release, Online safety law to be strengthened to stamp out illegal content, 4 February 2022

168 HCWS675, Online Safety Update, 13 March 2022

169 HCWS590, Update on the Law Commission's Review of Modernising Communications Offences, 4 February 2022

170 Paragraph 41 of the Explanatory Notes (PDF)

- the person had no reasonable excuse for sending the message[171]

Clause 151 sets out the false communications offence, which would be committed if:

- a person sends a message conveying information that the person knows to be false
- the person intended the message to cause "non-trivial psychological or physical harm" to a likely audience
- the person had no reasonable excuse for sending the message

An individual is part of a "likely audience" for the clause 150 and 151 offences if it is reasonably foreseeable that the individual would encounter the message, or (in the online context) would encounter a subsequent message forwarding or sharing the content of the message.

Clauses 150 and 151 both include what has been described as a "press exemption".[172] This provides that the offences cannot be committed by defined press and media bodies,[173] or in connection with the showing to members of the public of a film that was made for cinema.

Clause 152 sets out the threatening communications offence, which would be committed if:

- a person sends a message conveying a threat of death or serious harm[174]
- the person intended an individual encountering the message to fear that the threat would be carried out, or was reckless as to whether such an individual would feat that the threat would be carried out

Clause 153 sets out how different aspects of the three new offences should be interpreted. In particular, "sending a message" would include sending, transmitting or publishing a communication (including an oral communication) by electronic means, or sending a letter or a thing of any other description. It would also be irrelevant whether the sender had

---

171 Clause 150(5) provides that one factor the court must consider (if relevant to the particular case) when assessing reasonable excuse is whether the message was a contribution to a matter of public interest

172 HCWS590, Update on the Law Commission's Review of Modernising Communications Offences, 4 February 2022

173 The listed bodies are recognised news publishers (as defined in clause 50), those with licences under the Broadcasting Act 1990 or 1996 or section 8 of the Wireless Telegraphy Act 2006, or the providers of on-demand programme services (as defined in section 368A of the Communications Act 2003)

174 "Serious harm" is defined as serious injury amounting to grievous bodily harm within the meaning of the Offences against the Person Act 1861, rape, assault by penetration within the meaning of section 2 of the Sexual Offences Act 2003, or serious financial loss

created the content themselves – the offences could therefore also be committed by senders who forward or share other people's content.

Under **clause 154** the three new offences would also apply to acts done outside the United Kingdom, but only where the act is "done by a United Kingdom person", meaning an individual who is habitually resident in England and Wales or a body incorporated or constituted under the law of England and Wales.

The Joint Committee on the draft Online Safety Bill had recommended that the new communications offences be included on the face of the Bill as "illegal content".[175] However, the Government has not accepted this recommendation, on the basis that "these offences rely heavily on a user's intent making it challenging for services to proactively identify this content, without significant additional context".[176]

'Cyberflashing'

Clause 156 would add a new section 66A to the Sexual Offences Act 2003, which would make it an offence for a person to intentionally send or give a photograph or film of any person's genitals to another person. The offence would only be committed where:

- the sender intended that the recipient would see the genitals and be caused alarm, distress or humiliation, or
- the sender's purpose was to obtain sexual gratification and they were reckless as to whether the recipient would be caused alarm, distress or humiliation

References to sending or giving would include sending an image by any means, electronically or otherwise, showing an image to another person, or placing an image for a particular person to find.

There has been some criticism of the offence including a requirement for the sender to have had a specific intention (to cause alarm, distress or humiliation) or motivation (to obtain sexual gratification, being reckless as to causing alarm, distress or humiliation), rather than being based on the recipient's lack of consent alone. For example, the End Violence Against Women Coalition has said it has "significant concerns" about the enforceability of the offence, given the difficulties in evidencing a perpetrator's intent to cause harm, and has argued that "the only relevant

[175] Joint Committee on the draft Online Safety Bill, Draft Online Safety Bill, HL Paper 129/HC 609, 14 December 2021, paras 126-127

[176] DCMS, Government response to the Joint Committee report on the draft Online Safety Bill, 17 March 2022, para 89

factor in this offence should be whether or not there was consent, given that we know image-based sexual abuse causes harm regardless of intention".[177]

However, the Law Commission considered that including a requirement for the sender to have a specific intent or motivation would avoid the risk of 'over-criminalising' the conduct the new offence aims to tackle:

> We have real sympathy with the argument that an absence of consent is common to all acts of cyberflashing (ie those communicated images we would want to criminalise). However, we are not persuaded that the touchstone of criminal wrongfulness lies in the absence of consent alone. The threshold of criminality for this sort of conduct must be higher than that.[178]

In a separate review the Law Commission has provisionally proposed an offence of taking or sharing an intimate image of another person without their consent (with no requirement to prove any additional motivation).[179] However, the Law Commission considered that the infringement of sexual autonomy resulting from cyberflashing "would seem to be a different order of harm than the violation of sexual autonomy that is the non-consensual taking or sharing of an intimate image", and it did not therefore believe that "a non-consent approach to criminal liability is the best way to criminalise cyberflashing".[180]

177 End Violence Against Women Coalition, Women and girls failed by government's Online Safety Bill, 17 March 2022

178 Law Commission, Modernising Communications Offences: A final report (PDF), Law Com No 399, July 2021, para 6.108

179 Law Commission, Taking, making and sharing intimate images without consent [accessed 1 April 2022]

180 Law Commission, Modernising Communications Offences: A final report (PDF), Law Com No 399, July 2021, paras 6.108-9

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