HOUSE OF LORDS Library Briefing

Online Safety Bill
HL Bill 87 of 2022–23

Author: Emily Haves
Date published: 25 January 2023

The House of Lords is scheduled to debate the Online Safety Bill at second reading on 1 February 2023.

The bill would establish a regulatory framework for certain online services. These include user-to-user services, such as Facebook, and search services, such as Google. The government's aim in introducing the bill is "to make Britain the best place in the world to set up and run a digital business, while simultaneously ensuring that Britain is the safest place in the world to be online".

The bill would place duties of care on both regulated user-to-user service providers and regulated search service providers. The regulated service providers would have duties relating to, among other things:

- illegal content
- protecting children
- user empowerment
- content of democratic importance, news publisher content and journalistic content
- freedom of expression and privacy
- fraudulent advertising

The bill would establish Ofcom as the regulator. It would give Ofcom the power to levy fines against non-compliant providers, and would make senior managers liable to imprisonment for not complying with a direction to provide Ofcom with information.

Following changes in government leadership, several clauses were recommitted to a House of Commons public bill committee in late 2022. There, among other changes, clauses that would have imposed adult safety duties of care on regulated providers were removed. The Labour Party opposed this change.

The government has said it will bring forward amendments on several different issues in the House of Lords. These include:

- new offences relating to intimate images and promoting self-harm
- criminal sanctions for senior managers of non-compliant providers
- promotion of small boat crossings

Table of Contents

Table of contents

1. Background

1.1 Green and white papers

Online safety has a significant history of policy consideration and parliamentary scrutiny.

In October 2017 the government published its internet safety strategy, a green paper setting out its objectives on online safety.[1] It said it wanted to "make Britain the best place in the world to set up and run a digital business, while simultaneously ensuring that Britain is the safest place in the world to be online". The government proposed three principles to underpin its internet safety goals:

- What is unacceptable offline should be unacceptable online.
- All users should be empowered to manage online risks and stay safe.
- Technology companies have a responsibility to their users.

In April 2019 the government published its online harms white paper.[2] In it, the government said the digital economy needed a new regulatory framework to improve citizens' safety online. It said this was because of the prevalence of illegal and harmful content online and the level of public concern about online harms. The white paper set out the government's online regulation proposals and sought responses to questions about them.

The government said it would "tackle content or activity that harms individual users, particularly children, or threatens our way of life in the UK".[3] Threatening content would include that which either undermined either national or "our shared rights, responsibilities and opportunities to foster integration". It argued that social media companies could promote disinformation by using algorithms to show users one type of content rather than a range of opinions.

The white paper proposed a new statutory duty of care, supported by a regulatory framework, to make companies take responsibility for the safety of their users and tackle harm caused by content or activity on their services.[4] This regulatory framework would be enforced by an independent regulator and would apply to companies that allowed users to discover user-generated content or interact with each other online. The regulator would have the power to levy fines.

---

[1] HM Government, 'Internet safety strategy—green paper', October 2017, p 3.
[2] HM Government, 'Online harms white paper', April 2019, CP 57.
[3] As above, p 6.
[4] As above, p 7.

Issues raised by respondents to the consultation included:[5]

- the potential impact on freedom of expression online
- businesses that would be in scope
- the identity of the regulator
- a potential 'one size fits all' approach to transparency, and the material costs for companies associated with reporting
- transparency
- ensuring the regulator acted proportionately
- enforcement
- protection of children

In its response to the consultation, published in December 2020, the government confirmed its intention to introduce legislation to regulate online content, protect freedom of expression and uphold media freedom.[6] It said the legislation's principal aims would be tackling illegal activity taking place online and preventing children from being exposed to inappropriate material. The government said it would also address other types of harm that spread online, such as untruths about vaccines and pro-anorexia content. It emphasised the legislation would include a complaints mechanism and would focus on the biggest, highest risk online companies.

The government response confirmed that it intended to appoint Ofcom as the relevant regulator.[7]

1.2 Law Commission report

As part of the government's online harms strategy, the Law Commission undertook a review into the criminal law governing harmful, threatening and false communications. It also examined the criminal law around encouraging and assisting serious self-harm, and cyberflashing (defined as sending an unsolicited photograph or film of genitals).

In its report published in July 2021, the Law Commission noted that the "revolution" in online communications presented increased scope for harm.[8] It added the criminal law was "ill-suited" to addressing these harms. It argued that the threshold of criminality for existing offences was too low when applied to the online space, whereas other forms of harmful

[5] Department for Digital, Culture, Media and Sport and Home Office, 'Online harms white paper: Initial consultation response', updated 15 December 2020.
[6] Department for Digital, Culture, Media and Sport and Home Office, 'Online harms white paper: Full government response to the consultation', December 2020, CP 354, pp 3–4.
[7] As above, p 5.
[8] Law Commission, 'Reform of the communications offences', July 2021.

communication online had no or insufficient criminal sanction. It also said that existing laws that most directly addressed online communications were "overlapping, ambiguous and could be unclear for online users, technology companies and law enforcement agencies alike". Finally, it said current offences were broad enough that they could constitute a disproportionate interference in the right to freedom of expression.

The Law Commission recommended the following new or reformed criminal offences:

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

The commission also recommended the introduction of a new offence of sending flashing images to a person known to have epilepsy ('epilepsy trolling'). However, it did not make recommendations on the precise form of the offence.

The Law Commission responded to views that lack of consent should be sufficient for cyberflashing to count as an offence, regardless of motive. The commission stated it believed lack of consent alone was too low a bar for a criminal offence and that an offender should have had to be reckless as to an adverse, harmful consequence of sending the image. It said:

> 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.[9]

1.3 Draft bill

The government published a draft bill in May 2021. It proposed imposing duties of care on user-to-user services (services where content uploaded by one user can be encountered by another) and on search services. It also

[9] Law Commission, 'Modernising communications offences: A final report', July 2021, HC 547 of session 2021–22, p 187.

introduced the concept of 'category 1 services'. These would be determined by the number of users and the functionality of the platform. Category 1 user-to-user services would have a responsibility to tackle content that was legal but posed a risk of harm.[10] Other regulated providers would only have duties about illegal content and protecting children.

Regulated providers classed as category 2A and 2B would have to file annual transparency reports. Category 2A and 2B providers would be determined based on number of users and, for user-to-user services, on functionality.

The draft bill included duties about rights of freedom of expression and privacy for all user-to-user providers and search service providers. Category 1 user-to-user service providers would also have duties relating to protecting content of democratic importance and protecting journalistic content.

1.3.1 Joint committee on the draft bill and government response

A joint committee examined the draft bill. Reporting in December 2021, the committee praised the draft bill as a "key step forward for democratic societies to bring accountability and responsibility to the internet".[11] It said this was necessary because "self-regulation of online services has failed". The committee argued that algorithms amplified false, divisive and harmful content to maximise engagement. As a result, it argued, major online service providers could not be considered neutral publishers.

The committee's report discussed whether the bill's proposed provisions to tackle privately shared child sexual exploitation and abuse (CSEA) content could require service providers to compromise their end-to-end encryption.[12] All other provisions in the draft bill would only apply to content shared publicly. The committee said it was unclear how the privacy and freedom benefits of end-to-end encryption could be balanced with online safety requirements.

In its response, published in March 2022, the government said it supported encryption but it "should not be rolled out without appropriate safety mitigations, for example, the ability to continue to detect known CSEA imagery".[13] It said it was supporting the development of technologies that could detect CSEA within end-to-end encrypted environments while respecting user privacy.

---

[10] Department for Digital, Culture, Media and Sport and Home Office, 'Draft Online Safety Bill', 12 May 2021.
[11] Joint Committee on the Draft Online Safety Bill, 'Draft Online Safety Bill', 14 December 2021, HL Paper 129 of session 2021–22, p 3.
[12] As above, p 74.
[13] HM Government, 'Government response to the report of the Joint Committee on the draft Online Safety Bill', March 2022, CP 640, p 15.

While it supported the draft bill, the committee made recommendations intended to strengthen its provisions. Among its other conclusions, the committee agreed with the Law Commission's proposed new offences.

In response to the committee's report, the government made changes to the bill that incorporated 66 of the committee's recommendations.[14] These included:[15]

- introducing a new standalone duty requiring category 1 and category 2A services to take action to minimise the likelihood of fraudulent adverts being published on their service
- including priority offences on the face of the bill
- requiring category 1 services to ensure adult users were given the option to verify their identity, and tools to have more control over the legal content they saw and who they interacted with
- adding new harm-based, false and threatening communications offences and a new offence of cyberflashing, as recommended by the Law Commission
- requiring all service providers that published or displayed pornographic content on their services to prevent children from accessing this content
- no longer deferring the power to bring in criminal sanctions for failures to comply with information notices
- amending the definition of harmful content accessed by adults so that all categories of such content would be voted on by Parliament
- adding provisions for Ofcom to recommend the use of tools for content moderation, user profiling and behaviour identification

The government said it would further consider whether to add new offences of hoax calling, encouraging self-harm and epilepsy trolling.[16]

2. The bill

The bill is wide-ranging and complex. The bill as introduced in the House of Lords comprises 212 clauses organised in 12 parts, with 17 schedules. This section provides a summary of the main provisions in the bill. It should be read in conjunction with the explanatory notes to the bill, the impact

[14] HM Government, 'Government response to the report of the Joint Committee on the draft Online Safety Bill', March 2022, CP 640, p 6.
[15] Department for Digital, Culture, Media and Sport, 'Online Safety Bill: Factsheet', updated 18 January 2023.
[16] HM Government, 'Government response to the report of the Joint Committee on the Draft Online Safety Bill', March 2022, CP 640, p 6.

assessments and delegated powers memorandum:

- Explanatory notes
- Department for Digital, Culture, Media and Sport, 'Impact assessment', 31 January 2022; Regulatory Policy Committee, 'The Online Safety Bill', 18 February 2022; Department for Digital, Culture, Media and Sport, 'Overview of expected impact of changes to the Online Safety Bill', 18 January 2023
- Department for Culture, Media and Sport, 'Memorandum from the Department for Digital, Culture, Media and Sport and the Home Office to the Delegated Powers and Regulatory Reform Committee', 20 January 2023

This briefing brings together provisions by theme, rather than covering all clauses sequentially.

2.1 Extent and application

The bill would extend to England and Wales, Scotland and Northern Ireland with some exceptions:

- The false and threatening communications offences and the cyberflashing offence would extend to England and Wales only.
- The flashing images offence would extend to England and Wales and Northern Ireland only.

Internet policy is reserved. However, elements of the bill would interact with devolved competencies and the UK government would need to seek legislative consent from the devolved administrations concerning areas where the bill would confer powers to them.[17]

The bill would have extra territorial application. It would apply to providers of regulated services based outside the UK.

The new false and threatening communications offences would apply to an act committed outside the UK if done by:

- a person who was habitually resident in England and Wales, or
- a body incorporated or constituted under the law of England and Wales.

[17] Explanatory notes, p 16.

The offence of sending flashing images to someone with epilepsy would apply to an act committed outside the UK if done by:

- a person who was habitually resident in England and Wales or Northern Ireland, or
- a body incorporated or constituted under the law of England and Wales or Northern Ireland.

2.2 Parts 1 and 2

Part 1 contains one clause providing an overview of the different parts of the bill.

Part 2 provides key definitions. It defines a user-to-user service as one in which content generated by one user could be encountered by another user. It defines a search service as an internet service that is or includes a search engine.

User-to-user services and search services would become regulated services if they had "links with the UK" and were not exempt as provided for under schedules 1 or 2. A service would be deemed to have links with the UK if it had "a significant number" of UK users or UK users were a target market. In addition, a service would become regulated if it was capable of being used in the UK and there were reasonable grounds to believe there was a material risk of significant harm to individuals in the UK presented by content on the service.

Schedules 1 and 2 provide exemptions for, among other things, internal business services, services provided by public bodies and services provided by education or childcare institutions.

2.3 Part 3: Duties of care

2.3.1 Definitions

Chapter 7 of part 3 contains definitions relating to part 3 on duties of care.

Clause 49 defines different types of content. While user-generated content is anything shared on a service by a user that could be encountered by another user, regulated user-generated content would exclude emails, SMS and MMS messages, one-to-one live aural communications, comments and reviews on provider content and news publisher content, among other things.

Search content is defined in clause 51. The definition of search content excludes, among other things, paid-for advertisements and content on the

websites of "recognised news publishers".

A recognised news publisher is defined in clause 50. Conditions include material being subject to editorial control and having a procedure for handling complaints.

Clauses 7 and 21 define the scope of the duties of care for user-to-user services and search services respectively. These state, among other things, that the duties apply to the services only as far as the services operate in and relate to the UK.

The table below summarises the duties of care the bill would impose and which entities they would apply to.

Duty	**Who**
Illegal content risk assessment	Regulated user-to-user services (clause 8)
	Regulated search services (clause 22)
Illegal content	Regulated user-to-user services (clause 9)
	Regulated search services (clause 23)
Content reporting	Regulated user-to-user services (clause 16)
	Regulated search services (clause 26)
Complaints procedures	Regulated user-to-user services (clause 17)
	Regulated search services (clause 27)
Freedom of expression and privacy	Regulated user-to-user services (clause 18(2), (3))
	Regulated search services (clause 28)
	Category 1 providers (clause 18(4), (6) and (7))
Record keeping and review	Regulated user-to-user services (clause 19)
	Regulated search services (clause 29)
Children's risk assessment	Regulated user-to-user services (clause 10)
	Regulated search services (clause 24)

Protect children's online safety	Regulated user-to-user services (clause 11)
	Regulated search services (clause 25)
Empower adult users	Category 1 providers (clause 12)
Protect content of democratic importance	Category 1 providers (clause 13)
Protect news publisher content	Category 1 providers (clause 14)
Protect journalistic content	Category 1 providers (clause 15)

2.3.2 Illegal content duties

The illegal content duties have elements referring both to illegal content and priority illegal content. Illegal content is defined in clause 53 as content amounting to something that is already an offence, if the victim is an individual. Certain exclusions would apply.

Priority offences and priority illegal content relate to terrorism (content that amounts to an offence specified in schedule 5), child sexual exploitation and abuse (content that amounts to an offence specified in schedule 6), and content relating to other offences that are set out in schedule 7. The offences in schedule 7 are existing offences relating to:

- assisting suicide
- threats to kill
- public order offences, harassment, stalking and fear or provocation of violence
- drugs and psychoactive substances
- firearms and other weapons
- assisting illegal immigration
- sexual exploitation
- sexual images
- proceeds of crime
- fraud
- financial services
- attempting or conspiring to commit an offence specified in this schedule

Both regulated providers of user-to-user services and regulated providers of search services would have to carry out an illegal content risk assessment to determine the risk of users encountering illegal content.

Regulated providers of user-to-user services and regulated providers of search services would have differing safety duties about illegal content under

the bill. Clause 9 would provide that regulated providers of user-to-user services must take or use proportionate measures to:

- prevent individuals from encountering priority illegal content by means of their service
- mitigate and manage the risk of the service being used for the commission or facilitation of a priority offence
- mitigate and manage the risk of harm to individuals

They would also have a duty to use proportionate systems and processes designed to minimise the length of time for which any priority illegal content was present and take down such content when the provider became aware of it.

Clause 9(5) would impose a duty on regulated providers of user-to-user services to include in the terms of service how individuals would be protected from illegal content, separately addressing different types of priority illegal content. They would have to ensure these were applied consistently.

Under clause 23, regulated providers of search services would also have a duty to mitigate and manage the risks of harm to individuals as identified in the illegal content risk assessment. They would have a duty to use proportionate systems and processes to minimise the risk of individuals encountering search content which was priority illegal content or other illegal content the provider knew about.

Regulated search service providers would have to make a publicly available statement about their policies and procedures to protect users from illegal content and apply them consistently.

2.3.3 Protecting children

The bill would establish different types of content that could be harmful to children:

- primary priority content harmful to children
- priority content harmful to children
- content that is harmful to children

Primary priority content harmful to children and priority content harmful to children would be designated in regulations by the secretary of state. Content that is harmful to children is defined as other content which presents a material risk of significant harm to an appreciable number of children in the UK.

In a statement on 7 July 2022 the then secretary of state for digital, culture, media and sport, Nadine Dorries, gave examples of types of content the government might designate in regulations: [18]

> Primary priority content (which children would have to be prevented from encountering altogether):
>
> - pornography
> - content promoting self-harm (with some content which may be designated as priority content, for example content focused on recovery from self-harm)
> - content promoting eating disorders (with some content which may be designated as priority content, for example content focused on recovery from an eating disorder)
> - legal suicide content (with some content which may be designated as priority content, for example content focused on recovery)
>
> Priority content (which companies would need to ensure was age appropriate for their child users):
>
> - online abuse, cyberbullying and harassment
> - harmful health content (including health and vaccine misinformation and disinformation)
> - content depicting or encouraging violence

Clauses 30 and 31 would require all regulated user-to-user services and regulated search services ('part 3 services') to undertake a children's access assessment. To conclude that it was not possible for children to access a service, or part of it, the provider would have to have systems or processes in place so that children were "not normally able to access the service or that part of it". These systems could include age verification or another means of age assurance.

If the children's access assessment concluded that children could access the service, the service would be treated as 'likely to be accessed by children' for the purposes of the bill under clause 32. The clause also sets out further situations in which a service could be deemed likely to be accessed by children.

Regulated user-to-user service providers and regulated search service providers that were likely to be accessed by children would both have a duty to carry out children's risk assessments under clause 10 and 24 respectively.

---

[18] House of Commons, 'Written statement: Online safety update', 7 July 2022, HCWS194.

These would have to identify the risk of harm to children from content on the provider's service and how the design and operation of the service could reduce or increase the risks.

Under clause 11 regulated user-to-user services likely to be accessed by children would have to mitigate and manage the risk of harm to children in different age groups as identified by the risk assessment. They would also have to mitigate the risk of harm to children in different age groups presented by content that was harmful to children. Clause 25 would impose the same requirements on search services.

The regulated user-to-user services likely to be accessed by children would have to use systems and processes to prevent children of any age from encountering primary priority content. They would also have to protect children in age groups judged to be at risk from other harmful content from encountering it. Regulated search services would have to minimise these risks.

Regulated user-to-user services would have to set out in their terms of service how they would prevent children from encountering different types of harmful content and to apply these terms of service consistently. Regulated search services would have to include provisions about the subject in a publicly available statement and would have to apply these provisions consistently.

2.3.4 User empowerment

Clause 12 would place obligations on category 1 services to empower users.

Category 1 services are defined as regulated user-to-user services that meet certain conditions that would be specified by the proposed regulator, Ofcom. Ofcom has stated that these would be "the highest reach user-to-user services with the highest risk functionalities".[19]

The bill would also place particular obligations on category 2A and 2B providers. Ofcom describes these as "the highest reach search services" and "other services with potentially risky functionalities or other factors" respectively.[20] Under clause 86 Ofcom would set thresholds for these categories.

The empowerment duties aim to enable adult users to increase their control over content they could encounter. The bill would require category 1 services to include features which adult users could use to increase their

[19] Ofcom, 'Online Safety Bill: Ofcom's roadmap to regulation', 6 July 2022, p 5.
[20] As above.

control over certain types of content. These are:

- content promoting suicide or an act of deliberate self-injury
- content promoting an eating disorder or behaviours associated with an eating disorder
- abusive content targeting characteristics of race, religion, sex, sexual orientation, disability or gender reassignment
- content inciting hatred against people of a particular race, religion, sex or sexual orientation, who have a disability or who have the characteristic of gender reassignment

Category 1 service providers would also have to give users the option to prevent non-verified users from interacting with their content and to enable systems to reduce the likelihood of encountering content by non-verified users. Category 1 providers would have to give all adult users the option to verify their identity.

Michelle Donelan, secretary of state for digital, culture, media and sport, has stated that the user empowerment duties, together with the duty to remove illegal content and duty for providers to act in accordance with their terms of service, constitute a "triple shield" of tools to protect and empower adults.[21]

2.3.5 Content of democratic importance, news publisher content and journalistic content

Category 1 providers would also have duties relating to content of democratic importance, news publisher content and journalistic content.

Clause 13 would require category 1 service providers to ensure their systems and processes considered the importance of the free expression of content of democratic importance. In particular, they would have to consider this when making decisions about how to treat such content and whether to take action against a user who had posted it. Content would be deemed to be of democratic importance if it appeared to be "specifically intended to contribute to democratic political debate in the UK".

Clause 15 would make the same provision concerning the free expression of journalistic content. It would also require category 1 service providers to have an expedited complaints procedure available for decisions about content the user considered to be journalistic.

[21] House of Commons, 'Written statement: Online Safety Bill—update', 29 November 2022, HCWS397.

Clause 14 would require category 1 service providers to take certain steps before taking action about content from recognised news publishers on their services.

2.3.6 Content reporting

Under clauses 16 and 26, regulated user-to-user services and regulated search services would have to have duties to have systems and processes in place for people to easily report content they deemed to be illegal. Regulated services likely to be accessed by children would have the same obligation for content that was harmful to children.

2.3.7 Complaints procedures

Clause 17 would require regulated user-to-user services to have a complaints procedure for 'relevant complaints'. Clause 27 would do the same for regulated search services.

Relevant complaints include those concerning:

- illegal content
- non-compliance with duties on illegal content, content reporting or freedom of expression and privacy
- user content being taken down or users being restricted from using the service (user-to-user services)
- content not appearing or being given a lower priority in search results because of action taken to comply with measures in the bill (search services)

In addition, relevant complaints for services likely to be accessed by children would be those concerning:

- content harmful to children
- non-compliance with a duty on children's online safety
- content taken down or removed from, or appearing lower down in, search results because of actions taken to comply with certain duties in the bill
- complaints related to incorrect assessment of a user's age

2.3.8 Freedom of expression and privacy

Both regulated user-to-user services and regulated search services would have duties concerning freedom of expression and privacy under clauses 18 and 28.

All regulated services would have to have particular regard to the importance of protecting users' right to freedom of expression within the law when putting in place safety measures and policies. They would also have to have particular regard to protecting users from breaches of any laws relating to privacy.

Category 1 services would have a duty to carry out an impact assessment to consider how safety measures and policies would affect privacy and the right to freedom of expression within the law. Such services would have to provide a publicly available statement about the steps taken in response to such an impact assessment.

2.3.9 Record-keeping and review duties

Clauses 19 and 29 would impose record-keeping and review duties on regulated user-to-user services and regulated search services. These would require the services to keep a record of risk assessments and measures taken to comply with relevant duties. They would also require the services to review compliance with relevant duties after major changes.

2.3.10 Fraudulent advertising

Clauses 33 and 34 would impose a new duty on category 1 and 2A service providers to prevent paid-for fraudulent adverts appearing on their services.

To be fraudulent the advertisement would have to be an offence under clause 35 and not be regulated user-generated content. The offences under clause 35 relate to financial services and certain offences under the Fraud Act 2006, including fraud by false representation and by abuse of position.

2.3.11 Codes of practice

Chapter 6 of part 3 concerns codes of practice and guidance. These would be issued by Ofcom.

Draft codes of practice would have to be submitted to the secretary of state. The secretary of state could direct Ofcom to modify a draft code for reasons of public policy or, in the case of terrorism or CSEA content, for reasons of national security or public safety. Draft codes would have to be laid before Parliament, which would have 40 days (not including days when Parliament was dissolved, prorogued or adjourned for more than four days) to resolve not to approve the draft.

The bill states that Ofcom would have to provide guidance for providers of part 3 services on how to comply with their duties under the bill.

2.4 Part 4: Other duties for providers of regulated user-to-user services and regulated search services

In addition to the duty to enable users to verify their identity, chapter 2 of part 4 would place an obligation on UK regulated user-to-user services and regulated search services to operate systems that ensured they reported any detected CSEA content to the National Crime Agency (NCA). This requirement would extend to non-UK providers of regulated user-to-user services and regulated search services for all UK-linked CSEA content. A person would commit an offence if they provided false information in relation to this obligation.

Further provisions relating to CSEA content are in chapter 5 of part 7. These would give Ofcom powers to require providers to use certain technologies to identify CSEA content. This would include content communicated privately.

Chapter 3 stipulates that providers of category 1 services could only act against users (by taking down their content, restricting their access to content or suspending or banning them from the service) in accordance with their terms of service. However, this duty would not prevent a provider from taking down content to comply with other duties in the bill or because a user had committed an offence by posting the content.

Chapter 4 concerns transparency reports. It would provide that category 1, 2A and 2B service providers would have to produce an annual transparency report. Ofcom would produce guidance about the content of these reports.

2.5 Part 5: Pornographic content

Part 5 would place a duty on internet services displaying their own pornographic content to ensure that children would not normally be able to encounter that content. This could be by using age verification.

2.6 Part 6: Fees

Part 6 would require providers of regulated services to pay fees to Ofcom. These fees would be determined by reference to the provider's qualifying worldwide revenue and any other factors that Ofcom considered appropriate.

Schedule 10 would provide for Ofcom to recover its initial costs for setting up its online safety functions from providers of regulated services.

2.7 Part 7: Ofcom's powers and duties

2.7.1 Duties

Part 7 would amend Ofcom's general duties under the Communications Act 2003 to include a duty to secure "adequate protection of citizens from harm presented by content on regulated services". It also contains provisions relating to categories of part 3 service providers, and would place other duties on Ofcom.

2.7.2 Information notices

Part 7 would give Ofcom a power to require service providers and others associated with them to provide information to enable Ofcom to exercise its online safety functions. Ofcom would do this by issuing an information notice. Ofcom would be able to require, in its information notice, the service provider to name a senior manager responsible for complying with the notice.

Once Ofcom had given a provider an information notice, it would be an offence for a person (the definition of which under clause 207 would include companies and other organisations) not to comply with that notice. A senior manager would also commit an offence if the entity they were a senior manager of did not comply with the notice and the individual had not taken all reasonable steps to make sure the entity did not commit that offence. The bill would also provide for other information offences.

A person convicted of an information offence would be liable to a fine or imprisonment, or both.

2.7.3 Notices to deal with terrorism content or CSEA content

Chapter 5 would give Ofcom the power to give a notice to a regulated user-to-user service or a regulated search service provider to deal in a certain way with terrorism or CSEA content.

Clause 110(2) would apply to regulated user-to-user services. For terrorism content, Ofcom could require the provider to use accredited technology to identify and take down publicly communicated terrorism content on its service. A provider could also be required to prevent individuals from encountering this content if communicated publicly on its service.

For CSEA content, Ofcom could require the provider to use accredited technology to identify and take down CSEA content, whether communicated publicly or privately. A provider could also be required to prevent individuals from encountering this content by means of its service, whether communicated publicly or privately.

Clause 110(3) would apply to regulated search services. These providers could be required to use accredited technology to identify terrorism and CSEA content and ensure it did not appear on their services.

2.7.3 Ofcom's enforcement powers

The bill would give Ofcom the power to act against a provider of a regulated service if it deemed the provider was not complying with requirements to fulfil duties under the act. Ofcom would be able to require a person or organisation (as defined in clause 207) to pay a penalty in relation to this non-compliance. The maximum amount for this penalty would be £18mn or 10% of qualifying worldwide revenue, as set out in schedule 13.

Ofcom would be able to apply to the courts for a service restriction order. This would require persons providing services or access to the non-compliant provider to implement 'business disruption measures' to restrict those services or access to the regulated service.

2.7.4 Committees, research and reports

Chapter 7 would require Ofcom to establish a committee on disinformation and misinformation. It would also impose requirements about research and reports.

2.8 Part 8: Appeals and super-complaints

Part 8 would provide that providers of regulated services could appeal Ofcom's decision about their inclusion in the register of categories of service. They would also be able to appeal against certain notices and enforcement action.

Eligible entities, the criteria for which would be set out in regulations, would be able to bring super complaints if a regulated service risked causing significant harm, significantly adversely affecting the right to freedom of expression, or otherwise having a significant adverse impact on users or the public.

2.9 Part 9: Secretary of state's functions

Part 9 would allow the secretary of state to make a statement setting out the government's strategic priorities on online safety. The secretary of state would have to consult Ofcom before making a draft statement and then lay the draft before Parliament, where it would be subject to the negative resolution procedure.

The secretary of state could also issue directions and guidance to Ofcom on

various matters. Part 9 would require the secretary of state to report annually on its functions under the bill and to review the legislation's operation.

2.10 Part 10: Communications offences

Part 10 would provide for new offences of false communications, threatening communications, sending or showing flashing images electronically (epilepsy trolling) and sending photographs or films of genitals (cyberflashing).

Clause 160 would create a new offence of sending a message conveying information a person knew to be false ('false communications offence'). To be an offence, a person would have had to intend the message to cause "non-trivial psychological or physical harm". A person convicted of this offence would be liable for imprisonment or a fine. A news publisher could not commit a false communications offence.

The bill would also create a new offence of sending a message conveying a threat of death or serious harm, under clause 162. A person would have to have intended an individual encountering a message to fear a threat would be carried out and "was reckless as to whether an individual encountering the message would fear that the threat would be carried out".

Clause 164 would create a new offence of sending or showing flashing images electronically. For an offence to have been committed a sender must have known or suspected a recipient had epilepsy, or it must have been reasonably foreseeable that a person with epilepsy would see the image and the person sending it intended harm to come to that person as a result.

Clause 167 would amend the Sexual Offences Act 2003 to create an offence of sending a photograph or film of genitals. To qualify as an offence, the person sending a photograph or film would have to intend that another person would be caused alarm, distress or humiliation by seeing it, or be sending it for their own sexual gratification and be reckless as to whether the other person would be caused alarm, distress or humiliation.

3. House of Commons stages

The government first introduced the bill in the House of Commons on 17 March 2022 in the 2021–22 session. It received a second reading on 19 April 2022 and was then carried over into the 2022–23 session.[22] It had its first and second readings on 11 May 2022 and was considered in public bill committee over nine days in May and June 2022.[23] It then had a day of

[22] HC Hansard, 19 April 2022, cols 93–137.

[23] House of Commons, 'Votes and proceedings', 11 May 2022; House of Commons Public Bill Committee, 'Online Safety Bill: Compilation of committee debates so far', 29 June 2022.

report stage in July 2022 and a further day in December 2022.[24]

After the second day of report stage some clauses of the bill were recommitted. These were considered over a further three committee sittings in December 2022 and one report stage debate, on 17 January 2022. The bill received its third reading in the House of Commons on 17 January 2022 and was introduced in the House of Lords on 18 January 2022.

3.1 Major changes in the Commons

This section provides an overview of the major changes to the bill that occurred during its House of Commons stages up to and including its second committee stage on 13 and 15 December 2022. For more detailed information about these stages, please see the House of Commons Library briefing 'Online Safety Bill: Commons stages' (12 January 2023). The bill's second report stage, concerning the recommitted clauses, is discussed in section 3.2 below.

During the bill's first committee stage in June 2022 the committee agreed to add a new government schedule to the bill to enable Ofcom to recover its initial costs by charging fees to service providers.[25] The committee also agreed a government amendment requiring Ofcom to consult the Information Commissioner's Office before publishing guidance on using its enforcement powers.[26] No opposition amendments were agreed.

The first day of report stage took place on 12 July 2022. Government amendments were added to the bill relating to journalistic content, adult safety duties, and illegal content duties:

- Amendments to part 3 would provide that category 1 companies would have additional obligations before removing news publisher content on their platforms and assess the impact of their safety duties on journalistic content.[27] Other amendments to do with journalistic content were also added.
- Further amendments to part 3 were intended to clarify that the bill would require providers to improve transparency about content than was harmful to adults, rather than require them to remove it.[28]

---

[24] HC Hansard, 12 July 2022, cols 147–270 and HC Hansard, 5 December 2022, cols 22–162.
[25] House of Commons Public Bill Committee, 'Online Safety Bill', 23 June 2022, session 2022–23, 15th sitting, col 604.
[26] House of Commons Public Bill Committee, 'Online Safety Bill', 14 June 2022, session 2022–23, 9th sitting, col 359.
[27] HC Hansard, 12 July 2022, cols 219 and 226.
[28] As above, col 163.

- Changes to service design requirements in the bill stipulate that providers would have to mitigate the risk of their services being used to commit or facilitate the commission of a priority offence. These changes were designed to tackle 'breadcrumbing', in which offenders initiate contact with children on one platform but the offence occurs on another platform or offline.[29]
- Amendments were agreed that changed how providers would be required to determine whether content was illegal.[30]

During the second day of the first report stage, on 5 December 2022, further government amendments were added:

- a new offence of epilepsy trolling
- removal of the proposed new harmful communications offence and the proposed repeal of existing harmful communications offences

During three additional committee stage sittings government amendments were made concerning adult safety duties, user empowerment and the removal or restriction of legal content:[31]

- The committee agreed changes to remove adult safety duties from the bill, termed 'legal but harmful' by some.
- New user empowerment tools were added.
- Amendments were agreed that would require category 1 providers to only remove or restrict access to legal content if doing so was consistent with their terms of service.

Introducing the amendments, Parliamentary Under Secretary of State for Tech and the Digital Economy Paul Scully said the government wanted to remove clauses relating to adult safety duties "to protect free speech and remove any possibility that the bill could cause tech companies to censor legal content".[32] In response, Shadow Minister for Digital, Culture, Media and Sport Alex Davies-Jones said the amendments would mean the remaining provisions would "not constitute robust enough regulation to deal with the threat that these platforms present".[33]

The government said that, taken together, its amendments would create a

---

[29] Department for Culture, Media and Sport, 'Fact sheet on changes to the illegal content duties within the Online Safety Bill', 23 August 2022.
[30] As above.
[31] House of Commons Public Bill Committee, 'Online Safety Bill', 13 December 2022, 1st sitting, col 26.
[32] As above, col 24.
[33] As above, col 28.

"fairer, simpler and we believe more effective mechanism called the triple shield, which will focus on user choice, consumer rights and accountability whilst protecting freedom of expression".[34]

Other government amendments, concerning Ofcom guidance and categorising services, were also made.

3.2 Second report stage

On 17 January 2023 the House of Commons met to consider on report those clauses that had been recommitted. These were clauses concerning:

- safety duties protecting children
- safety duties protecting adults
- duties about content reporting and complaints procedures
- duties about freedom of expression and privacy
- the relationship between duties and codes of practice
- interpretation
- transparency reports
- Ofcom's powers

Only these recommitted clauses could be considered at the second report stage.

Government amendments consequential on the changes to remove the provisions on content that was legal but harmful to adults were made without division.

One Labour and one SNP amendment were defeated on division.

Labour's Alex Davies-Jones moved several new clauses, the aim of which was to re-insert some provisions to protect adults from 'legal but harmful' content. Ms Jones argued that the government's removal of clauses relating to legal but harmful content was "a major weakening" of the bill and that "important sections that would have put protections in place to prevent content such as health and foreign-state disinformation, the promotion of self-harm, and online abuse and harassment from being actively pushed and promoted were rapidly removed by the government".[35] She said the government's alternative proposal, to filter out harmful content, was "unworkable" and asked "exactly how will this bill do anything to keep adults safe online?".

---

[34] House of Commons, 'Written statement: Online Safety Bill—update', 29 November 2022, HCWS397.
[35] HC Hansard, 17 January 2023, col 274.

Ms Davies-Jones also spoke to Labour's new clause 4, which would have enabled Ofcom to set minimum standards for terms of service for safety duties relating to adults and society. She said this would "ensure that the platforms are not able to avoid safety duties by changing their terms and conditions".[36] The new clause was defeated on division by 310 votes to 242.

An SNP amendment was also defeated on division. This would have changed clause 12 so that the features adult users could use to control content they saw would be enabled by default. Kirsty Blackman, SNP shadow spokesperson for the Cabinet Office, said that this would enable people to avoid harmful or unsafe content while protecting the right to free speech. She said:[37]

> People can say whatever they want as long as it is below that bar of illegality, but we should not have to read it. We should not have to read abuse that is pointed toward minority groups. We should start from the position of having the safest option on.

The Labour Party supported the amendment. Ms Davies-Jones said that the opposition had concerns about the government's approach to allowing adults to control the content they encountered, but that given the changes the government had made the filtering features should be enabled by default.[38] The amendment was defeated on division by 316 votes to 237.

4. Government commitments to revisit issues in the Lords

The government made commitments to revisit several issues during the Lords stages of the bill.

4.1 New offence of encouraging self-harm

In a written statement on 29 November 2022, Michelle Donelan announced the government intended to bring an amendment to the bill in the House of Lords that would create a new offence of encouraging serious self-harm. She wrote:

> I am aware of particular concerns around content online which encourages vulnerable people to self-harm. While the child safety duties in the bill will protect children, vulnerable adults may remain at risk of exposure to this abhorrent content. I am therefore committing to making the encouragement of self-harm illegal. The government will bring forward in this bill proposals to create an offence of sending a

[36] HC Hansard, 17 January 2023, col 277.
[37] As above, col 284.
[38] As above, col 278.

> communication that encourages serious self-harm via an amendment in the House of Lords. This new offence will ensure that trolls sending such messages to a person, regardless of the recipient's age, face the consequences for their vile actions.[39]

On the second day of the bill's first report stage, in December 2022, Labour's Ms Davies-Jones said the opposition supported the government's plans to criminalise the encouragement of self-harm.[40]

The Molly Rose Foundation, a suicide-prevention charity aimed at young people, said it also supported the proposed new offence.[41] The charity was established by the friends and family of Molly Russell, a 14-year-old girl who took her own life after viewing images promoting suicide and self-harm.[42] In September 2022 a coroner ruled that content Molly had viewed relating to depression, self-harm and suicide "had contributed to her death in a more than minimal way".[43] The foundation said the proposed new offence would be a "significant move" but that it was important that other 'harmful but legal' content was also brought within scope of the bill.[44]

David Davis (Conservative MP for Haltemprice and Howden), who had supported the government's removal of the legal but harmful provisions, also supported the proposal to make the encouragement of self-harm an offence. He said that rather than asking if legal content was harmful, the right question was "is it harmful enough to be made illegal?".[45] He added that "obviously, self-harm material is harmful enough to be made illegal".

4.2 New intimate images offence

The government said it would also introduce in the House of Lords a new offence concerning the taking and sharing of intimate images. This would be part of the government's plan to introduce a package of laws on the issue, as recommended by the Law Commission.[46]

---

[39] House of Commons, 'Written statement: Online Safety Bill—update', 29 November 2022, HCWS397.
[40] HC Hansard, 5 December 2022, col 54.
[41] Molly Rose Foundation, 'Proposal to introduce a new criminal offence of "encouraging self-harm"', November 2022.
[42] Molly Rose Foundation, 'Molly Russell: A father's journey', accessed 19 January 2023.
[43] Leigh Day, 'Molly Russell's family call for urgent changes to online safety', 30 September 2022.
[44] Molly Rose Foundation, 'Proposal to introduce a new criminal offence of "encouraging self-harm"', November 2022.
[45] HC Hansard, 5 December 2022, col 78.
[46] House of Commons, 'Written statement: Intimate images abuse offences', 25 November 2022, HCWS388.

The Law Commission's report 'Taking, making and sharing of intimate images without consent', published in July 2022, recommended five new offences related to intimate images.[47] It recommended a "base offence" of taking or sharing an intimate image without consent and three more serious offences:

- an offence of taking or sharing an intimate image without consent with the intention of causing the victim humiliation, alarm or distress
- an offence of taking or sharing an intimate image without consent with the intention that the image will be looked at for the purpose of obtaining sexual gratification
- an offence of threatening to share an intimate image

The Law Commission also recommended the creation of an offence of installing equipment to commit an offence.

In her November 2022 written statement, Ms Donelan said the government would bring forward an amendment to the Online Safety Bill in the Lords to criminalise the sharing of people's intimate images without their consent.[48] She said the government would separately bring forward a package of additional laws to tackle other abusive behaviour, including the installation of equipment to take or record images of someone without their consent.

The Labour Party has said it supports this proposal.[49]

4.3 Controlling or coercive behaviour as a priority offence

The secretary of state's statement on 29 November 2022 said the government would introduce amendments to tackle violence against women and girls. The statement said these would:

- List controlling or coercive behaviour as a priority offence. This is an offence that disproportionately impacts women and girls—listing this as a priority offence means companies will have to take proactive measures to tackle this content, therefore strengthening the protections for women and girls under the bill.
- Name the victims' commissioner and the domestic abuse commissioner as statutory consultees for the codes of practice, to ensure that they are consulted by Ofcom ahead of drafting

[47] Law Commission, 'Taking, making and sharing intimate images without consent', July 2022.
[48] House of Commons, 'Written statement: Online Safety Bill—update', 29 November 2022, HCWS397.
[49] HC Hansard, 5 December 2022, col 54.

and amending the codes of practice.[50]

The Labour Party had previously introduced amendments at committee and report stage which would have added content that constituted, encouraged or promoted violence against women and girls to priority illegal content.[51] Both amendments were defeated on division.

4.4 Criminal liability for senior managers

A backbench Conservative-proposed new clause that would have created a new offence for senior managers attracted cross-party support ahead of the bill's second report stage. The new clause would have made senior managers criminally liable if a provider failed to comply with the safety duties protecting children and failure was attributable to the manager's consent, connivance or neglect. The maximum penalty would have been two years imprisonment or a fine, or both.[52] The shadow culture secretary, Lucy Powell, said the Labour Party would support the amendment.[53]

In the 2019 online harms white paper the government said it was exploring possible options for senior manager liability.[54] It said this could involve personal liability for civil fines, "or could even extend to criminal liability".

In its response to the consultation, the government said the industry had highlighted the risk of potential negative impacts on the attractiveness of the UK tech sector if criminal liability for failing to comply were included in the bill.[55] Instead, it said it would "reserve the right to introduce criminal sanctions for senior managers who fail to respond fully, accurately and in a timely manner to information requests from the online harms regulator". This measure is now in the bill.

Ahead of the second report stage debate, Ms Donelan said the government "was not ruling out" changing the bill to create the new offence and would "take a sensible approach" when considering the amendment.[56]

Speaking to the proposed new clause, one of its leading proponents,

---

[50] House of Commons, 'Written statement: Online Safety Bill—update', 29 November 2022, HCWS397.
[51] House of Commons Public Bill Committee, 'Online Safety Bill', 28 June 2022, session 2022–23, 16th sitting, col 650 and HC Hansard, 12 July 2022, col 173.
[52] HC Hansard, 17 January 2023, col 267.
[53] Adam Forrest, 'Labour vows to hand "weak" Rishi Sunak first defeat over Online Safety Bill', Independent, 16 January 2023.
[54] HM Government, 'Online harms white paper', April 2019, CP 57, p 60.
[55] Department for Digital, Culture, Media and Sport and Home Office, 'Online harms white paper: Full government response to the consultation', 15 December 2020, CP 354, p 75.
[56] BBC News, 'Online Safety Bill changes "not ruled out"—culture secretary', 13 January 2023.

Sir William Cash (Conservative MP for Stone), argued criminal liability was essential to keep children safe:

> In a nutshell, we must be able to threaten tech bosses with jail. There is precedent for that—jail sentences for senior managers are commonplace for breaches of duties across a great range of UK legislation. That is absolutely and completely clear, and as a former shadow attorney general, I know exactly what the law is on this subject. I can say this: we must protect our children and grandchildren from predatory platforms operating for financial gain on the internet.[57]

He and other members, including joint-proposer Miriam Cates (Conservative MP for Penistone and Stocksbridge) highlighted that similar penalties were already in place in the financial and construction sectors.

Responding on behalf of the government, Mr Scully said ministers were sympathetic to the aims of the amendment.[58] He said the government would work with members to bring forward an effective amendment on the issue in the Lords, in lieu of the proposed amendment:

> We are committed to ensuring that children are safe online, so we will work with those members and others to bring to the other place an effective amendment that delivers our shared aims of holding people accountable for their actions in a way that is effective and targeted at child safety, while ensuring that the UK remains an attractive place for technology companies to invest and grow.

Mr Scully said the government would base its amendment on legislation recently passed in the Republic of Ireland and would introduce individual criminal liability for failure to comply with the notice to end contravention:

> While the amendment will not affect those who have acted in good faith to comply in a proportionate way, it will give the act additional teeth—as we have heard—to deliver the change that we all want, and ensure that people are held to account if they fail to protect children properly.

4.5 Small boats

The government also said it would bring an amendment in the Lords to address the promotion of small boat crossings online. An amendment brought by Natalie Elphicke (Conservative MP for Dover) and Sir John Hayes (Conservative MP for South Holland and The Deepings) aimed to make

[57] HC Hansard, 17 January 2023, col 300.
[58] As above, col 312.

regulated user-to-user service providers introduce systems to protect children from encountering content encouraging them to cross the English Channel in an unsafe boat.[59]

Speaking to the amendment, Ms Elphicke said it would introduce a requirement to remove content that could result in serious harm to or death of a child while crossing the English Channel in a small boat.[60] She argued that social media was partly responsible for this content being circulated:

> The risk of harm or death from channel crossings is very real. Four children have drowned in the past 15 months, with many more harmed through exposure to petrol and saltwater burns and put in danger here and abroad by organised crime and people traffickers. Social media is playing a direct role in this criminal enterprise. It must be brought to book, and the videos and other content that encourage such activity must be taken down.

In response, the government said it would act on the issue, though it would not accept the amendment. It said it would add section 2 of the Modern Slavery Act 2015 to the list of priority offences in the bill.[61] Section 2 makes it an offence to arrange or facilitate the travel of another person, including through recruitment, with a view to their exploitation.

The government said it would also add section 24 of the Immigration Act 1971 to the priority offences list.[62] The minister explained that although the offences in section 24 could not be committed online, the bill would provide that encouraging or enabling these offences would be illegal under the bill:

> Therefore aiding, abetting, counselling and conspiring in those offences by posting videos of people crossing the channel that show the activity in a positive light could be an offence that is committed online and therefore fall within what is priority illegal content. The result of this amendment would therefore be that platforms would have to proactively remove that content.

4.6 Definition of recognised news publisher

During the bill's first committee stage, Kim Leadbeater (Labour MP for Batley and Spen), introduced an amendment that would have required news publishers to belong to an approved regulator to take advantage of the

---

[59] HC Hansard, 17 January 2023, col 270.
[60] As above, col 299.
[61] As above, col 314.
[62] As above.

exemptions in the bill.[63] She said this was necessary because as currently drafted any organisation could declare themselves a news publisher by "obtaining a UK address, jotting down a standards code on the back of an envelope and inviting readers to send an email if they have any complaints". She said organisations could take advantage of this exemption to "distribute profoundly damaging and dangerous material designed to promote extremist ideologies and stir up hatred".[64] She also said that "hostile state actors" could take advantage of the exemption to spread disinformation, mentioning state-sponsored news outlet Russia Today (RT).

Chris Philp, then parliamentary under secretary of state at the Department for Digital, Culture, Media and Sport, said the clause, as drafted, had "been looked at in some detail over a number of years and debated with news publishers and others".[65] He said it was "the best attempt that we have so far collectively been able to come up with to provide a definition of a news publisher that does not infringe on press freedom". On foreign organisations, however, he said the government would look into amending the bill:

> In relation to hostile states, such as Russia, I do not think anyone in the UK press would have the slightest objection to us finding ways to tighten up on such matters.[66]

Speaking on the issue in the bill's first report stage, the then minister, Damian Collins, said the government had committed to changing the definition of recognised news provider in the Lords so that sanctioned entities, such as RT, could not benefit from its protections.[67]

Speaking on behalf of the Labour Party, Ms Davies-Jones said she welcomed the government's plan to exclude Russia Today from the recognised news publisher exemption, but argued this measure did not go far enough because "disinformation outlets rarely have the profile of Russia Today".[68]

During the bill's third reading in the House of Commons Michelle Donelan confirmed the government's plans to make the changes.[69]

---

[63] House of Commons Public Bill Committee, 'Online Safety Bill', 14 June 2022, session 2022–23, 10th sitting, col 372.
[64] As above, col 371.
[65] As above, col 372.
[66] As above, col 373.
[67] HC Hansard, 12 July 2022, col 162.
[68] As above, col 172.
[69] HC Hansard, 17 January 2023, col 329.

4.7 Other proposed changes

4.7.1 Release of data following the death of a child

During the first and second report stage debates in the Commons, members asked the government to consider an amendment Baroness Kidron (Crossbench) had indicated she would table to the bill when the bill was considered in the Lords.[70] This would require social media companies to provide coroners with access to data in cases where the death of a child may have been related to social media and other online activities.

It has been reported that this amendment would give Ofcom powers to ensure parents and coroners have access to social media data within a timeframe set by the coroner.[71] A further amendment, it is reported, would require service providers to preserve information as soon as a notice was served and for a senior manager to testify at an inquest if required.[72]

This proposal is supported by the Molly Rose Foundation, as well as other bereaved families.[73] Molly Russell's family have said it took five years for them and the coroner investigating Molly's death to get access her social media data.

In relation to the proposal to give coroners access to data, Mr Scully has said that the government would "happily work with Baroness Kidron, and others, and look favourably on changes where they are necessary".[74]

Speaking to the BBC, Baroness Kidron said she would also look to table an amendment to increase the scope of the bill so that types of online platform other than user-to-user and search services, such as blogs, would be included.[75]

4.7.2 Changes proposed under previous leadership

In a statement on 7 July 2022 the then secretary of state for digital, culture, media and sport, Nadine Dorries, outlined areas where the government intended to make changes to the bill. She said the government would bring

---

[70] BBC Radio 4, 'Today in Parliament', 2 December 2022, 2:39

[71] Charles Hymas, 'Let parents see dead children's social media: Move to give Ofcom power', Telegraph (£), 18 January 2023.

[72] Dan Milmo, 'UK families call for easier access to deceased children's social media history', Guardian, 5 December 2022.

[73] Mark Sellman, 'Online Safety Bill: Bereaved families back law forcing big tech to release children's data', Times (£), 5 December 2022.

[74] HC Hansard, 17 January 2023, col 313.

[75] BBC Radio 4, 'Westminster hour', 15 January 2023, 37:25.

forward these amendments in the Lords if necessary. Of those proposed changes, two have not been made and relate to provisions still in the bill:[76]

- changes to the secretary of state's power to require Ofcom to modify a draft of a code of practice for reasons of public policy
- requirements for the highest-risk companies to publish a summary of their illegal and child safety risk assessments and to submit these to Ofcom

[76] House of Commons, 'Written statement: Online Safety Bill—update for report stage', 7 July 2022, HCWS193.

About the Library

A full list of Lords Library briefings is available on the Library's website.

The Library publishes briefings for all major items of business debated in the House of Lords. The Library also publishes briefings on the House of Lords itself and other subjects that may be of interest to members.

Library briefings are produced for the benefit of Members of the House of Lords. They provide impartial, authoritative, politically balanced information in support of members' parliamentary duties. They are intended as a general briefing only and should not be relied on as a substitute for specific advice.

Every effort is made to ensure that the information contained in Lords Library briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

Disclaimer

Authors are available to discuss the contents of the briefings with Members of the House of Lords and their staff but cannot advise members of the general public.

Any comments on Library briefings should be sent to the Head of Research Services, House of Lords Library, London SW1A 0PW or emailed to hlresearchservices@parliament.uk.