PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

ONLINE SAFETY BILL

Sixth Sitting

Tuesday 7 June 2022

(Afternoon)

CONTENTS

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Saturday 11 June 2022

The Committee consisted of the following Members:

Chairs: Sir Roger Gale, † Christina Rees

† Ansell, Caroline *(Eastbourne)* (Con)
† Bailey, Shaun *(West Bromwich West)* (Con)
† Blackman, Kirsty *(Aberdeen North)* (SNP)
† Carden, Dan *(Liverpool, Walton)* (Lab)
† Davies-Jones, Alex *(Pontypridd)* (Lab)
† Double, Steve *(St Austell and Newquay)* (Con)
† Fletcher, Nick *(Don Valley)* (Con)
† Holden, Mr Richard *(North West Durham)* (Con)
† Keeley, Barbara *(Worsley and Eccles South)* (Lab)
† Leadbeater, Kim *(Batley and Spen)* (Lab)
† Miller, Dame Maria *(Basingstoke)* (Con)
† Mishra, Navendu *(Stockport)* (Lab)
† Moore, Damien *(Southport)* (Con)
† Nicolson, John *(Ochil and South Perthshire)* (SNP)
† Philp, Chris *(Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport)*
Russell, Dean *(Watford)* (Con)
† Stevenson, Jane *(Wolverhampton North East)* (Con)

Katya Cassidy, Kevin Maddison, Seb Newman, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 7 June 2022

(Afternoon)

[Christina Rees *in the Chair*]

Online Safety Bill

2 pm

The Chair: Welcome back. I have a few announcements. I have been reassured that we will have no transmission problems this afternoon, and apparently the audio of this morning's sitting is available if Members want to listen to it. I have no objections to Members taking their jackets off, because it is rather warm this afternoon. We are expecting a Division in the main Chamber at about 4 o'clock, so we will suspend for 15 minutes if that happens.

Kirsty Blackman (Aberdeen North) (SNP): I am sorry, Ms Rees, but I am afraid that I cannot hear you very well.

The Chair: I will shout a bit in that case.

Clause 8

Illegal content risk assessment duties

Amendment proposed (this day): 10, in clause 8, page 6, line 33, at end insert—

"(4A) A duty to publish the illegal content risk assessment and proactively supply this to OFCOM."—*(Alex Davies-Jones.)*

This amendment creates a duty to publish an illegal content risk assessment and supply it to Ofcom.

Question again proposed, That the amendment be made.

The Chair: I remind the Committee that with this we are discussing the following:

Amendment 14, in clause 8, page 6, line 33, at end insert—

"(4A) A duty for the illegal content risk assessment to be approved by either—

(a) the board of the entity; or, if the organisation does not have a board structure,

(b) a named individual who the provider considers to be a senior manager of the entity, who may reasonably be expected to be in a position to ensure compliance with the illegal content risk assessment duties, and reports directly into the most senior employee of the entity."

This amendment seeks to ensure that regulated companies' boards or senior staff have responsibility for illegal content risk assessments.

Amendment 25, in clause 8, page 7, line 3, after the third "the" insert "production,".

This amendment requires the risk assessment to take into account the risk of the production of illegal content, as well as the risk of its presence and dissemination.

Amendment 19, in clause 8, page 7, line 14, at end insert—

"(h) how the service may be used in conjunction with other regulated user-to-user services such that it may—

(i) enable users to encounter illegal content on other regulated user-to-user services, and

(ii) constitute part of a pathway to harm to individuals who are users of the service, in particular in relation to CSEA content."

This amendment would incorporate into the duties a requirement to consider cross-platform risk.

Clause stand part.

Amendment 20, in clause 9, page 7, line 30, at end insert—

", including by being directed while on the service towards priority illegal content hosted by a different service;".

This amendment aims to include within companies' safety duties a duty to consider cross-platform risk.

Amendment 26, in clause 9, page 7, line 30, at end insert—

"(aa) prevent the production of illegal content by means of the service;".

This amendment incorporates a requirement to prevent the production of illegal content within the safety duties.

Amendment 18, in clause 9, page 7, line 35, at end insert—

"(d) minimise the presence of content which reasonably foreseeably facilitates or aids the discovery or dissemination of priority illegal content, including CSEA content."

This amendment brings measures to minimise content that may facilitate or aid the discovery of priority illegal content within the scope of the duty to maintain proportionate systems and processes.

Amendment 21, in clause 9, page 7, line 35, at end insert—

"(3A) A duty to collaborate with other companies to take reasonable and proportionate measures to prevent the means by which their services can be used in conjunction with other services to facilitate the encountering or dissemination of priority illegal content, including CSEA content,".

This amendment creates a duty to collaborate in cases where there is potential cross-platform risk in relation to priority illegal content and CSEA content.

Clause 9 stand part.

Amendment 30, in clause 23, page 23, line 24, after "facilitating" insert—

"the production of illegal content and".

This amendment requires the illegal content risk assessment to consider the production of illegal content.

Clause 23 stand part.

Amendment 31, in clause 24, page 24, line 2, after "individuals" insert "producing or".

This amendment expands the safety duty to include the need to minimise the risk of individuals producing certain types of search content.

Clause 24 stand part.

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Chris Philp): It is a great pleasure to serve under your chairmanship, Ms Rees, and I am glad that this afternoon's Committee proceedings are being broadcast to the world.

Before we adjourned this morning, I was in the process of saying that one of the challenges with public publication of the full risk assessment, even for larger companies, is that the vulnerabilities in their systems, or the potential opportunities to exploit those systems for criminal purposes, would then be publicly exposed in a way that may not serve the public interest, and that is a reason for not requiring complete disclosure of everything.

However, I draw the Committee's attention to the existing transparency provisions in clause 64. We will come on to them later, but I want to mention them now, given that they are relevant to amendment 10. The transparency duties state that, once a year, Ofcom must serve notice on the larger companies—those in categories 1, 2A and 2B—requiring them to produce a transparency report. That is not a power for Ofcom—it is a requirement. Clause 64(1) states that Ofcom

"must give every provider…a notice which requires the provider to produce…(a 'transparency report')."

The content of the transparency report is specified by Ofcom, as set out in subsection (3). As Members will see, Ofcom has wide powers to specify what must be included in the report. On page 186, schedule 8—I know that we will debate it later, but it is relevant to the amendment—sets out the scope of what Ofcom can require. It is an extremely long list that covers everything we would wish to see. Paragraph 1, for instance, states:

"The incidence of illegal content, content that is harmful to children and priority content that is harmful to adults on a service."

Therefore, the transparency reporting requirement—it is not an option but a requirement—in clause 64 addresses the transparency point that was raised earlier.

Amendment 14 would require a provider's board members or senior manager to take responsibility for the illegal content risk assessment. We agree with the Opposition's point. Indeed, we agree with what the Opposition are trying to achieve in a lot of their amendments.

Alex Davies-Jones (Pontypridd) (Lab): Vote for them, then.

Chris Philp: There is a "but" coming. We think that, in all cases apart from one, the Bill as drafted already addresses the matter. In the case of amendment 14, the risk assessment duties as drafted already explicitly require companies to consider how their governance structures may affect the risk of harm to users arising from illegal content. Ofcom will provide guidance to companies about how they can comply with those duties, which is very likely to include measures relating to senior-level engagement. In addition, Ofcom can issue confirmation decisions requiring companies to take specific steps to come into compliance. To put that simply, if Ofcom thinks that there is inadequate engagement by senior managers in relation to the risk assessment duties, it can require—it has the power to compel—a change of behaviour by the company.

I come now to clause 9—I think this group includes clause 9 stand part as well. The shadow Minister has touched on this. Clause 9 contains safety duties in relation to—

The Chair: Order. Minister, I do not think we are doing clause 9. We are on clause 8.

Chris Philp: I think the group includes clause 9 stand part, but I will of course be guided by you, Ms Rees.

The Chair: No, clause 9 is separate.

Chris Philp: Very well; we will debate clause 9 separately. In that case, I will move on to amendments 19 and 20, which seek to address cross-platform risk. Again, we completely agree with the Opposition that cross-platform risk is a critical issue. We heard about it in evidence. It definitely needs to be addressed and covered by the Bill. We believe that it is covered by the Bill, and our legal advice is that it is covered by the Bill, because in clause 8 as drafted—*[Interruption.]* Bless you—or rather, I bless the shadow Minister, following Sir Roger's guidance earlier, lest I inadvertently bless the wrong person.

Clause 8 already includes the phrase to which I alluded previously. I am talking about the requirement that platforms risk-assess illegal content that might be encountered

"by means of the service".

That is a critical phrase, because it means not just on that service itself; it also means, potentially, via that service if, for example, that service directs users onward to illegal content on another site. By virtue of the words,

"by means of the service",

appearing in clause 8 as drafted, the cross-platform risk that the Opposition and witnesses have rightly referred to is covered. Of course, Ofcom will set out further steps in the code of practice as well.

Dame Maria Miller (Basingstoke) (Con): I was listening very closely to what the Minister was saying and I was hoping that he might be able to comment on some of the evidence that was given, particularly by Professor Lorna Woods, who talked about the importance of risk assessments being about systems, not content. Would the Minister pick up on that point? He was touching on it in his comments, and I was not sure whether this was the appropriate point in the Bill at which to bring it up.

Chris Philp: I thank my right hon. Friend for raising that. The risk assessments and, indeed, the duties arising under this Bill all apply to systems and processes—setting up systems and processes that are designed to protect people and to prevent harmful and illegal content from being encountered. We cannot specify in legislation every type of harmful content that might be encountered. This is about systems and processes. We heard the Chairman of the Joint Committee on the draft Online Safety Bill, our hon. Friend the Member for Folkestone and Hythe (Damian Collins), confirm to the House on Second Reading his belief—his accurate belief—that the Bill takes a systems-and-processes approach. We heard some witnesses saying that as well. The whole point of this Bill is that it is tech-agnostic—to future-proof it, as hon. Members mentioned this morning—and it is based on systems and processes. That is the core architecture of the legislation that we are debating.

Amendments 25 and 26 seek to ensure that user-to-user services assess and mitigate the risk of illegal content being produced via functions of the service. That is covered, as it should be—the Opposition are quite right to raise the point—by the illegal content risk assessment and safety duties in clauses 8 and 9. Specifically, clause 8(5)(d), on page 7 of the Bill—goodness, we are only on page 7 and we have been going for over half a day already—requires services to risk-assess functionalities of their service being used to facilitate the presence of

[Chris Philp]

illegal content. I stress the word "presence" in clause 8(5)(d). Where illegal content is produced by a functionality of the service—for example, by being livestreamed—that content will be present on the service and companies must mitigate that risk. The objective that the Opposition are seeking to achieve, and with which we completely agree with, is covered in clause 8(5)(d) by the word "presence". If the content is present, it is covered by that section.

Kirsty Blackman: Specifically on that, I understand the point the hon. Gentleman is making and appreciate his clarification. However, on something such as Snapchat, if somebody takes a photo, it is sent to somebody else, then disappears immediately, because that is what Snapchat does—the photo is no longer present. It has been produced and created there, but it is not present on the platform. Can the Minister consider whether the Bill adequately covers all the instances he hopes are covered?

Chris Philp: The hon. Lady raises an interesting point about time. However, the clause 8(5)(d) uses the wording,

"the level of risk of functionalities of the service facilitating the presence or dissemination of illegal content"

and so on. That presence can happen at any time, even fleetingly, as with Snapchat. Even when the image self-deletes after a certain period—so I am told, I have not actually used Snapchat—the presence has occurred. Therefore, that would be covered by clause 8(5)(d).

Alex Davies-Jones: Will the Minister explain how we would be able to prove, once the image is deleted, that it was present on the platform?

Chris Philp: The question of proof is a separate one, and that would apply however we drafted the clause. The point is that the clause provides that any presence of a prohibited image would fall foul of the clause. There are also duties on the platforms to take reasonable steps. In the case of matters such as child sexual exploitation and abuse images, there are extra-onerous duties that we have discussed before, for obvious and quite correct reasons.

Kirsty Blackman: Will the Minister stress again that in this clause specifically he is talking about facilitating any presence? That is the wording that he has just used. Can he clarify exactly what he means? If the Minister were to do so, it would be an important point for the Bill as it proceeds.

The Chair: Order. Minister, before you continue, before the Committee rose earlier today, there was a conversation about clause 9 being in, and then I was told it was out. This is like the hokey cokey; it is back in again, just to confuse matters further. I was confused enough, so that point needs to be clarified.

Alex Davies-Jones: It is grouped, Chair. We were discussing clause 8 and the relevant amendments, then we were going to come back to clause 9 and the relevant amendments.

The Chair: Is that as clear as mud?

Chris Philp: I am happy to follow your direction, Ms Rees. I find that that is usually the wisest course of action.

I will speak to amendment 18, which is definitely on the agenda for this grouping and which the shadow Minister addressed earlier. It would oblige service providers to put in place systems and processes

"to minimise the presence of content which reasonably foreseeably facilitates or aids the discovery or dissemination of priority illegal content, including CSEA content."

The Government completely support that objective, quite rightly promoted by the Opposition, but it is set out in the Bill as drafted. The companies in scope are obliged to take comprehensive measures to tackle CSEA content, including where a service directs users on the first service to the second service.

Amendment 21, in a similar spirit, talks about cross-platform collaboration. I have already mentioned the way in which the referral of a user from one platform to another is within the scope of the Bill. Again, under its provisions, service providers must put in place proportionate systems and processes to mitigate identified cross-platform harms and, where appropriate, to achieve that objective service providers would be expected to collaborate and communicate with one another. If Ofcom finds that they are not engaging in appropriate collaborative behaviour, which means they are not discharging their duty to protect people and children, it can intervene. While agreeing completely with the objective sought, the Bill already addresses that.

2.15 pm

Amendments 30 and 31 are slightly different, as they try to put a duty on search services not to facilitate

"the production of illegal content".

Search services cannot produce or facilitate illegal content; all they can do is facilitate searches. Searching for illegal content using a search service is already covered by the Bill, and the end company that might be providing the illegal content would be covered as well if it is a user-to-user service. Everything that search services could reasonably be expected to do in this area is already covered by the duties imposed upon them.

Ms Rees, are we dealing with clauses 23 and 24 now, or later?

The Chair: They are in this group, so you may deal with them now.

Chris Philp: Obviously, I encourage the Committee to support those clauses standing part of the Bill. They impose duties on search services—we touched on search a moment ago—to assess the nature and risk to individuals of accessing illegal content via their services, and to minimise the risk of users encountering that illegal content. They are very similar duties to those we discussed for user-to-user services, but applied in the search context. I hope that that addresses all the relevant provisions in the group that we are debating.

Alex Davies-Jones: I am grateful for the opportunity to speak to amendments to clause 9 and to clauses 23 and 24, which I did not speak on earlier. I am also very grateful that we are being broadcast live to the world and welcome that transparency for all who might be listening.

On clause 9, it is right that the user-to-user services will be required to have specific duties and to take appropriate measures to mitigate and manage the risk of harm to individuals and their likelihood of encountering priority illegal content. Again, however, the Bill does not go far enough, which is why we are seeking to make these important amendments. On amendment 18, it is important to stress that the current scope of the Bill does not capture the range of ways in which child abusers use social networks to organise abuse, including to form offender networks. They post digital breadcrumbs that signpost to illegal content on third-party messaging apps and the dark web, and they share child abuse videos that are carefully edited to fall within content moderation guidelines. This range of techniques, known as child abuse breadcrumbing, is a significant enabler of online child abuse.

Our amendment would give the regulator powers to tackle breadcrumbing and ensure a proactive upstream response. The amendment would ensure that tens of millions of interactions with accounts that actively enable the discovery and sharing of child abuse material will be brought into regulatory scope. It will not leave that as ambiguous. The amendment will also ensure that companies must tackle child abuse at the earliest possible stage. As it stands, the Bill would reinforce companies' current focus only on material that explicitly reaches the criminal threshold. Because companies do not focus their approach on other child abuse material, abusers can exploit this knowledge to post carefully edited child abuse images and content that enables them to connect and form networks with other abusers. Offenders understand and can anticipate that breadcrumbing material will not be proactively identified or removed by the host site, so they are able to organise and link to child abuse in plain sight.

We all know that child abuse breadcrumbing takes many forms, but techniques include tribute sites where users create social media profiles using misappropriated identities of known child abuse survivors. These are used by offenders to connect with likeminded perpetrators to exchange contact information, form offender networks and signpost child abuse material elsewhere online. In the first quarter of 2021, there were 6 million interactions with such accounts.

Abusers may also use Facebook groups to build offender groups and signpost to child abuse hosted on third-party sites. Those groups are thinly veiled in their intentions; for example, as we heard in evidence sessions, groups are formed for those with an interest in children celebrating their 8th, 9th or 10th birthdays. Several groups with over 50,000 members remained alive despite being reported to Meta, and algorithmic recommendations quickly suggested additional groups for those members to join.

Lastly, abusers can signpost to content on third-party sites. Abusers are increasingly using novel forms of technology to signpost to online child abuse, including QR codes, immersive technologies such as the metaverse, and links to child abuse hosted on the blockchain. Given the highly agile nature of the child abuse threat and the demonstrable ability of sophisticated offenders to exploit new forms of technology, this amendment will ensure that the legislation is effectively futureproofed. Technological change makes it increasingly important that the ability of child abusers to connect and form offender networks can be disrupted at the earliest possible stage.

Turning to amendment 21, we know that child abuse is rarely siloed on a single platform or app. Well-established grooming pathways see abusers exploit the design features of social networks to contact children before they move communication across to other platforms, including livestreaming sites, as we have already heard, and encrypted messaging services. Offenders manipulate features such as Facebook's algorithmic friend suggestions to make initial contact with a large number of children. They can then use direct messages to groom them and coerce children into sending sexual images via WhatsApp. Similarly, as we heard earlier, abusers can groom children through playing videogames and then bringing them on to another ancillary platform, such as Discord.

The National Society for the Prevention of Cruelty to Children has shared details of an individual whose name has been changed, and whose case particularly highlights the problems that children are facing in the online space. Ben was 14 when he was tricked on Facebook into thinking he was speaking to a female friend of a friend, who turned out to be a man. Using threats and blackmail, he coerced Ben into sending abuse images and performing sex acts live on Skype. Those images and videos were shared with five other men, who then bombarded Ben with further demands. His mum, Rachel, said:

> "The abuse Ben suffered had a devastating impact on our family. It lasted two long years, leaving him suicidal.
>
> It should not be so easy for an adult to meet and groom a child on one site then trick them into livestreaming their own abuse on another app, before sharing the images with like-minded criminals at the click of a button.
>
> Social media sites should have to work together to stop this abuse happening in the first place, so other children do not have to go through what Ben did."

The current drafting of the Bill does not place sufficiently clear obligations on platforms to co-operate on the cross-platform nature of child abuse. Amendment 21 would require companies to take reasonable and proportionate steps to share threat assessments, develop proportionate mechanisms to share offender intelligence, and create a rapid response arrangement to ensure that platforms develop a coherent, systemic approach to new and emerging threats. Although the industry has developed a systemic response to the removal of known child abuse images, these are largely ad hoc arrangements that share information on highly agile risk profiles. The cross-platform nature of grooming and the interplay of harms across multiple services need to be taken into account. If it is not addressed explicitly in the Bill, we are concerned that companies may be able to cite competition concerns to avoid taking action.

Kirsty Blackman: On the topic of child abuse images, the hon. Member spoke earlier about livestreaming and those images not being captured. I assume that she would make the same point in relation to this issue: these live images may not be captured by AI scraping for them, so it is really important that they are included in the Bill in some way as well.

Alex Davies-Jones: I completely agree with the hon. Member, and appreciate her intervention. It is fundamental for this point to be captured in the Bill because, as we are seeing, this is happening more and more. More and

[Alex Davies-Jones]

more victims are coming forward who have been subject to livestreaming that is not picked up by the technology available, and is then recorded and posted elsewhere on smaller platforms.

Legal advice suggests that cross-platform co-operation is likely to be significantly impeded by the negative interplay with competition law unless there is a clear statutory basis for enabling or requiring collaboration. Companies may legitimately have different risk and compliance appetites, or may simply choose to hide behind competition law to avoid taking a more robust form of action.

New and emerging technologies are likely to produce an intensification of cross-platform risks in the years ahead, and we are particularly concerned about the child abuse impacts in immersive virtual reality and alternative-reality environments, including the metaverse. A number of high-risk immersive products are already designed to be platform-agnostic, meaning that in-product communication takes place between users across multiple products and environments. There is a growing expectation that these environments will be built along such lines, with an incentive for companies to design products in this way in the hope of blunting the ability of Governments to pursue user safety objectives.

Separately, regulatory measures that are being developed in the EU, but are highly likely to impact service users in the UK, could result in significant unintended safety consequences. Although the interoperability provisions in the Digital Markets Act are strongly beneficial when viewed through a competition lens—they will allow the competition and communication of multiple platforms—they could, without appropriate safety mitigations, provide new means for abusers to contact children across multiple platforms, significantly increase the overall profile of cross-platform risk, and actively frustrate a broad number of current online safety responses. Amendment 21 will provide corresponding safety requirements that can mitigate the otherwise significant potential for unintended consequences.

The Minister referred to clauses 23 and 24 in relation to amendments 30 and 31. We think a similar consideration should apply for search services as well as for user-to-user services. We implore that the amendments be made, in order to prevent those harms from occurring.

Chris Philp: I have already commented on most of those amendments, but one point that the shadow Minister made that I have not addressed was about acts that are essentially preparatory to acts of child abuse or the exchange of child sexual exploitation and abuse images. She was quite right to raise that issue as a matter of serious concern that we would expect the Bill to prevent, and I offer the Committee the reassurance that the Bill, as drafted, does so.

Schedule 6 sets out the various forms of child sexual exploitation and abuse that are designated as priority offences and that platforms have to take proactive steps to prevent. On the cross-platform point, that includes, as we have discussed, things that happen through a service as well as on a service. Critically, paragraph 9 of schedule 6 includes "inchoate offences", which means someone not just committing the offence but engaging in acts that are preparatory to committing the offence, conspiring to commit the offence, or procuring, aiding or abetting the commission of the offence. The preparatory activities that the shadow Minister referred to are covered under schedule 6, particularly paragraph 9.

Alex Davies-Jones: I thank the Minister for giving way. I notice that schedule 6 includes provision on the possession of indecent photographs of children. Can he confirm that that provision encapsulates the livestreaming of sexual exploitation?

Chris Philp: Yes, I can.

Question put, That the amendment be made.

The Committee divided: Ayes 5, Noes 9.

Division No. 2]

AYES

Carden, Dan	Leadbeater, Kim
Davies-Jones, Alex	
Keeley, Barbara	Mishra, Navendu

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	Stevenson, Jane
Holden, Mr Richard	

Question accordingly negatived.

2.30 pm

Amendment proposed: 14, in clause 8, page 6, line 33, at end insert:

"(4A) A duty for the illegal content risk assessment to be approved by either—

(a) the board of the entity; or, if the organisation does not have a board structure,

(b) a named individual who the provider considers to be a senior manager of the entity, who may reasonably be expected to be in a position to ensure compliance with the illegal content risk assessment duties, and reports directly into the most senior employee of the entity."—*(Alex Davies-Jones.)*

This amendment seeks to ensure that regulated companies' boards or senior staff have responsibility for illegal content risk assessments.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 3]

AYES

Blackman, Kirsty	Leadbeater, Kim
Carden, Dan	Mishra, Navendu
Davies-Jones, Alex	Nicolson, John
Keeley, Barbara	

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	Stevenson, Jane
Holden, Mr Richard	

Question accordingly negatived.

Amendment proposed: 25, in clause 8, page 7, line 3, after the third "the" insert "production,".—(*Alex Davies-Jones.*)

This amendment requires the risk assessment to take into account the risk of the production of illegal content, as well as the risk of its presence and dissemination.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 4]

AYES

Blackman, Kirsty	Leadbeater, Kim
Carden, Dan	Mishra, Navendu
Davies-Jones, Alex	
Keeley, Barbara	Nicolson, John

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	
Holden, Mr Richard	Stevenson, Jane

Question accordingly negatived.

Amendment proposed: 19, in clause 8, page 7, line 14, at end insert—

"(h) how the service may be used in conjunction with other regulated user-to-user services such that it may—

(i) enable users to encounter illegal content on other regulated user-to-user services, and

(ii) constitute part of a pathway to harm to individuals who are users of the service, in particular in relation to CSEA content."—(*Alex Davies-Jones.*)

This amendment would incorporate into the duties a requirement to consider cross-platform risk.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 5]

AYES

Blackman, Kirsty	Leadbeater, Kim
Carden, Dan	Mishra, Navendu
Davies-Jones, Alex	
Keeley, Barbara	Nicolson, John

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	
Holden, Mr Richard	Stevenson, Jane

Question accordingly negatived.

Amendment proposed: 17, in clause 8, page 7, line 14, at end insert—

'(5A) The duties set out in this section apply in respect of content which reasonably foreseeably facilitates or aids the discovery or dissemination of CSEA content." —*(Alex Davies-Jones.)*

This amendment extends the illegal content risk assessment duties to cover content which could be foreseen to facilitate or aid the discovery or dissemination of CSEA content.

The Chair: With this it will be convenient to discuss amendment 28, in clause 10, page 9, line 18, at end insert—

"(ba) matters relating to CSEA content including—

(i) the level of illegal images blocked at the upload stage and number and rates of livestreams of CSEA in public and private channels terminated; and

(ii) the number and rates of images and videos detected and removed by different tools, strategies and/or interventions."

This amendment requires the children's risk assessment to consider matters relating to CSEA content.

Barbara Keeley (Worsley and Eccles South) (Lab): As this is the first time I have spoken in the Committee, may I say that it is a pleasure to serve with you in the Chair, Ms Rees? I agree with my hon. Friend the Member for Pontypridd that we are committed to improving the Bill, despite the fact that we have some reservations, which we share with many organisations, about some of the structure of the Bill and some of its provisions. As my hon. Friend has detailed, there are particular improvements to be made to strengthen the protection of children online, and I think the Committee's debate on this section is proving fruitful.

Amendment 28 is a good example of where we must go further if we are to achieve the goal of the Bill and protect children from harm online. The amendment seeks to require regulated services to assess their level of risk based, in part, on the frequency with which they are blocking, detecting and removing child sexual exploitation and abuse content from their platforms. By doing so, we will be able to ascertain the reality of their overall risk and the effectiveness of their existing response.

The addition of livestreamed child sexual exploitation and abuse content not only acknowledges first-generation CSEA content, but recognises that livestreamed CSEA content happens on both public and private channels, and that they require different methods of detection.

Furthermore, amendment 28 details the practical information needed to assess whether the action being taken by a regulated service is adequate in countering the production and dissemination of CSEA content, in particular first-generation CSEA content. Separating the rates of terminated livestreams of CSEA in public and private channels is important, because those rates may vary widely depending on how CSEA content is generated. By specifying tools, strategies and interventions, the amendment would ensure that the systems in place to detect and report CSEA are adequate, and that is why we would like it to be part of the Bill.

Chris Philp: The Government support the spirit of amendments 17 and 28, which seek to achieve critical objectives, but the Bill as drafted delivers those objectives. In relation to amendment 17 and cross-platform risk, clause 8 already sets out harms and risks—including CSEA risks—that arise by means of the service. That means through the service to other services, as well as on the service itself, so that is covered.

Amendment 28 calls for the risk assessments expressly to cover illegal child sexual exploitation content, but clause 8 already requires that to happen. Clause 8(5) states that the risk assessment must cover the

"risk of individuals who are users of the service encountering…each kind of priority illegal content".

[Chris Philp]

If we follow through the definition of priority illegal content, we find all those CSEA offences listed in schedule 6. The objective of amendment 28 is categorically delivered by clause 8(5)(b), referencing onwards to schedule 6.

Kirsty Blackman: The amendment specifically mentions the level and rates of those images. I did not quite manage to follow through all the things that the Minister just spoke about, but does the clause specifically talk about the level of those things, rather than individual incidents, the possibility of incidents or some sort of threshold for incidents, as in some parts of the Bill?

Chris Philp: The risk assessments that clause 8 requires have to be suitable and sufficient; they cannot be perfunctory and inadequate in nature. I would say that suitable and sufficient means they must go into the kind of detail that the hon. Lady requests. More details, most of which relate to timing, are set out in schedule 3. Ofcom will be making sure that these risk assessments are not perfunctory.

Importantly, in relation to CSEA reporting, clause 59, which we will come to, places a mandatory requirement on in-scope companies to report to the National Crime Agency all CSEA content that they detect on their platforms, if it has not already been reported. Not only is that covered by the risk assessments, but there is a criminal reporting requirement here. Although the objectives of amendments 17 and 28 are very important, I submit to the Committee that the Bill delivers the intention behind them already, so I ask the shadow Minister to withdraw them.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 6]

AYES

Blackman, Kirsty	Leadbeater, Kim
Carden, Dan	Mishra, Navendu
Davies-Jones, Alex	
Keeley, Barbara	Nicolson, John

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	
Holden, Mr Richard	Stevenson, Jane

Question accordingly negatived.

Clause 8 ordered to stand part of the Bill.

Clause 9

SAFETY DUTIES ABOUT ILLEGAL CONTENT

The Chair: Amendments 20, 26, 18 and 21 to clause 9 have already been debated. Does the shadow Minister wish to press any of them to a vote?

Alex Davies-Jones: Amendments 20, 18 and 21.

Amendment proposed: 20, in clause 9, page 7, line 30, at end insert

", including by being directed while on the service towards priority illegal content hosted by a different service;"—*(Alex Davies-Jones.)*

This amendment aims to include within companies' safety duties a duty to consider cross-platform risk.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 7]

AYES

Blackman, Kirsty	Leadbeater, Kim
Carden, Dan	Mishra, Navendu
Davies-Jones, Alex	
Keeley, Barbara	Nicolson, John

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	
Holden, Mr Richard	Stevenson, Jane

Question accordingly negatived.

Amendment proposed: 18, in clause 9, page 7, line 35, at end insert—

"(d) minimise the presence of content which reasonably foreseeably facilitates or aids the discovery or dissemination of priority illegal content, including CSEA content."—*(Alex Davies-Jones.)*

This amendment brings measures to minimise content that may facilitate or aid the discovery of priority illegal content within the scope of the duty to maintain proportionate systems and processes.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 8]

AYES

Blackman, Kirsty	Leadbeater, Kim
Carden, Dan	Mishra, Navendu
Davies-Jones, Alex	
Keeley, Barbara	Nicolson, John

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	
Holden, Mr Richard	Stevenson, Jane

Question accordingly negatived.

2.45 pm

Amendment proposed: 21, in clause 9, page 7, line 35, at end insert—

"(3A) A duty to collaborate with other companies to take reasonable and proportionate measures to prevent the means by which their services can be used in conjunction with other services to facilitate the encountering or dissemination of priority illegal content, including CSEA content,"—*(Alex Davies-Jones.)*

This amendment creates a duty to collaborate in cases where there is potential cross-platform risk in relation to priority illegal content and CSEA content.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 9]

AYES

Blackman, Kirsty	Leadbeater, Kim
Carden, Dan	Mishra, Navendu
Davies-Jones, Alex	Nicolson, John
Keeley, Barbara	

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	Stevenson, Jane
Holden, Mr Richard	

Question accordingly negatived.

Clause 9 ordered to stand part of the Bill.

Clause 10

CHILDREN'S RISK ASSESSMENT DUTIES

Barbara Keeley: I beg to move amendment 15, in clause10, page 8, line 41, at end insert—

"(4A) A duty for the children's risk assessment to be approved by either—

(a) the board of the entity; or, if the organisation does not have a board structure,

(b) a named individual who the provider considers to be a senior manager of the entity, who may reasonably be expected to be in a position to ensure compliance with the children's risk assessment duties, and reports directly into the most senior employee of the entity."

This amendment seeks to ensure that regulated companies' boards or senior staff have responsibility for children's risk assessments.

The Chair: With this it will be convenient to discuss the following:

Amendment 11, in clause 10, page 9, line 2, at end insert—

"(5A) A duty to publish the children's risk assessment and proactively supply this to OFCOM."

This amendment creates a duty to publish the children's risk assessment and supply it to Ofcom.

Amendment 27, in clause 10, page 9, line 25, after "facilitating" insert "the production of illegal content and"

This amendment requires the children's risk assessment to consider the production of illegal content.

Clause 10 stand part.

Amendment 16, in clause 25, page 25, line 10, at end insert—

'"(3A) A duty for the children's risk assessment to be approved by either—

(a) the board of the entity; or, if the organisation does not have a board structure,

(b) a named individual who the provider considers to be a senior manager of the entity, who may reasonably be expected to be in a position to ensure compliance with the children's risk assessment duties, and reports directly into the most senior employee of the entity."

This amendment seeks to ensure that regulated companies' boards or senior staff have responsibility for children's risk assessments.

Amendment 13, in clause 25, page 25, line 13, at end insert—

"(4A) A duty to publish the children's risk assessment and proactively supply this to OFCOM."

This amendment creates a duty to publish the children's risk assessment and supply it to Ofcom.

Amendment 32, in clause 25, page 25, line 31, after "facilitating" insert "the production of illegal content and"

This amendment requires the children's risk assessment to consider risks relating to the production of illegal content.

Clause 25 stand part.

Barbara Keeley: I will speak to other amendments in this group as well as amendment 15. The success of the Bill's regulatory framework relies on regulated companies carefully risk-assessing their platforms. Once risks have been identified, the platform can concentrate on developing and implementing appropriate mitigations. However, up to now, boards and top executives have not taken the risk to children seriously. Services have either not considered producing risk assessments or, if they have done so, they have been of limited efficacy and failed to identify and respond to harms to children.

In evidence to the Joint Committee, Frances Haugen explained that many of the corporate structures involved are flat, and accountability for decision making can be obscure. At Meta, that means teams will focus only on delivering against key commercial metrics, not on safety. Children's charities have also noted that corporate structures in the large technology platforms reward employees who move fast and break things. Those companies place incentives on increasing return on investment rather than child safety. An effective risk assessment and risk mitigation plan can impact on profit, which is why we have seen so little movement from companies to take the measures themselves without the duty being placed on them by legislation.

It is welcome that clause 10 introduces a duty to risk-assess user-to-user services that are likely to be accessed by children. But, as my hon. Friend the Member for Pontypridd said this morning, it will become an empty, tick-box exercise if the Bill does not also introduce the requirement for boards to review and approve the risk assessments.

The Joint Committee scrutinising the draft Bill recommended that the risk assessment be approved at board level. The Government rejected that recommendation on the grounds thar Ofcom could include that in its guidance on producing risk assessments. As with much of the Bill, it is difficult to blindly accept promised safeguards when we have not seen the various codes of practice and guidance materials. The amendments would make sure that decisions about and awareness of child safety went right to the top of regulated companies. The requirement to have the board or a senior manager approve the risk assessment will hardwire the safety duties into decision making and create accountability and responsibility at the most senior level of the organisation. That should trickle down the organisation and help embed a culture of compliance across it. Unless there is a commitment to child safety at the highest level of the organisation, we will not see the shift in attitude that is urgently needed to keep children safe, and which I believe every member of the Committee subscribes to.

[Barbara Keeley]

On amendments 11 and 13, it is welcome that we have risk assessments for children included in the Bill, but the effectiveness of that duty will be undermined unless the risk assessments can be available for scrutiny by the public and charities. In the current version of the Bill, risk assessments will only be made available to the regulator, which we debated on an earlier clause. Companies will be incentivised to play down the likelihood of currently emerging risks because of the implications of having to mitigate against them, which may run counter to their business interests. Unless the risk assessments are published, there will be no way to hold regulated companies to account, nor will there be any way for companies to learn from one another's best practice, which is a very desirable aim.

The current situation shows that companies are unwilling to share risk assessments even when requested. In October 2021, following the whistleblower disclosures made by Frances Haugen, the National Society for the Prevention of Cruelty to Children led a global coalition of 60 child protection organisations that urged Meta to publish its risk assessments, including its data privacy impact assessments, which are a legal requirement under data protection law. Meta refused to share any of its risk assessments, even in relation to child sexual abuse and grooming. The company argued that risk assessments were live documents and it would not be appropriate for it to share them with any organisation other than the Information Commissioner's Office, to whom it has a legal duty to disclose. As a result, civil society organisations and the charities that I talked about continue to be in the dark about whether and how Meta has appropriately identified online risk to children.

Making risk assessments public would support the smooth running of the regime and ensure its broader effectiveness. Civil society and other interested groups would be able to assess and identify any areas where a company might not be meeting its safety duties and make full, effective use of the proposed super-complaints mechanism. It will also help civil society organisations to hold the regulated companies and the regulator, Ofcom, to account.

As we have seen from evidence sessions, civil society organisations are often at the forefront of understanding and monitoring the harms that are occurring to users. They have an in depth understanding of what mitigations may be appropriate and they may be able to support the regulator to identify any obvious omissions. The success of the systemic risk assessment process will be significantly underpinned by and reliant upon the regulator's being able to rapidly and effectively identify new and emerging harms, and it is highly likely that the regulator will want to draw on civil society expertise to ensure that it has highly effective early warning functions in place.

However, civil society organisations will be hampered in that role if they remain unable to determine what, if anything, companies are doing to respond to online threats. If Ofcom is unable to rapidly identify new and emerging harms, the resulting delays could mean entire regulatory cycles where harms were not captured in risk profiles or company risk assessments, and an inevitable lag between harms being identified and companies being required to act upon them. It is therefore clear that there is a significant public value to publishing risk assessments.

Amendments 27 and 32 are almost identical to the suggested amendments to clause 8 that we discussed earlier. As my hon. Friend the Member for Pontypridd said in our discussion about amendments 25, 26 and 30, the duty to carry out a suitable and sufficient risk assessment could be significantly strengthened by preventing the creation of illegal content, not only preventing individuals from encountering it. I know the Minister responded to that point, but the Opposition did not think that response was fully satisfactory. This is just as important for children's risk assessments as it is for illegal content risk assessments.

Online platforms are not just where abusive material is published. Sex offenders use mainstream web platforms and services as tools to commit child sexual abuse. This can be seen particularly in the livestreaming of child sexual exploitation. Sex offenders pay to direct and watch child sexual abuse in real time. The Philippines is a known hotspot for such abuse and the UK has been identified by police leads as the third-largest consumer of livestreamed abuse in the world. What a very sad statistic that our society is the third-largest consumer of livestreamed abuse in the world.

Ruby is a survivor of online sexual exploitation in the Philippines, although Ruby is not her real name; she recently addressed a group of MPs about her experiences. She told Members how she was trafficked into sexual exploitation aged 16 after being tricked and lied to about the employment opportunities she thought she would be getting. She was forced to perform for paying customers online. Her story is harrowing. She said:

> "I blamed myself for being trapped. I felt disgusted by every action I was forced to do, just to satisfy customers online. I lost my self-esteem and I felt very weak. I became so desperate to escape that I would shout whenever I heard a police siren go by, hoping somebody would hear me. One time after I did this, a woman in the house threatened me with a knife."

Eventually, Ruby was found by the Philippine authorities and, after a four-year trial, the people who imprisoned her and five other girls were convicted. She said it took many years to heal from the experience, and at one point she nearly took her own life.

It should be obvious that if we are to truly improve child protection online we need to address the production of new child abuse material. In the Bill, we have a chance to address not only what illegal content is seen online, but how online platforms are used to perpetrate abuse. It should not be a case of waiting until the harm is done before taking action.

Chris Philp: As the hon. Lady said, we discussed in the groupings for clauses 8 and 9 quite a few of the broad principles relating to children, but I will none the less touch on some of those points again because they are important.

On amendment 27, under clause 8 there is already an obligation on platforms to put in place systems and processes to reduce the risk that their services will be used to facilitate the presence of illegal content. As that includes the risk of illegal content being present, including that produced via the service's functionality, the terrible example that the hon. Lady gave is already covered by the Bill. She is quite right to raise that example, because

it is terrible when such content involving children is produced, but such cases are expressly covered in the Bill as drafted, particularly in clause 8.

Amendment 31 covers a similar point in relation to search. As I said for the previous grouping, search does not facilitate the production of content; it helps people to find it. Clearly, there is already an obligation on search firms to stop people using search engines to find illegal content, so the relevant functionality in search is already covered by the Bill.

Amendments 15 and 16 would expressly require board member sign-off for risk assessments. I have two points to make on that. First, the duties set out in clause 10(6)(h) in relation to children's risk assessments already require the governance structures to be properly considered, so governance is directly addressed. Secondly, subsection (2) states that the risk assessment has to be "suitable and sufficient", so it cannot be done in a perfunctory or slipshod way. Again, Ofcom must be satisfied that those governance arrangements are appropriate. We could invent all the governance arrangements in the world, but the outcome needs to be delivered and, in this case, to protect children.

Beyond governance, the most important things are the sanctions and enforcement powers that Ofcom can use if those companies do not protect children. As the hon. Lady said in her speech, we know that those companies are not doing enough to protect children and are allowing all kinds of terrible things to happen. If those companies continue to allow those things to happen, the enforcement powers will be engaged, and they will be fined up to 10% of their global revenue. If they do not sort it out, they will find that their services are disconnected. Those are the real teeth that will ensure that those companies comply.

Barbara Keeley: I know that the Minister listened to Frances Haugen and to the members of charities. The charities and civil society organisations that are so concerned about this point do not accept that the Bill addresses it. I cannot see how his point addresses what I said about board-level acceptance of that role in children's risk assessments. We need to change the culture of those organisations so that they become different from how they were described to us. He, like us, was sat there when we heard from the big platform providers, and they are not doing enough. He has had meetings with Frances Haugen; he knows what they are doing. It is good and welcome that the regulator will have the powers that he mentions, but that is just not enough.

3 pm

Chris Philp: I agree with the hon. Lady that, as I said a second ago, those platforms are not doing enough to protect children. There is no question about that at all, and I think there is unanimity across the House that they are not doing enough to protect children.

I do not think the governance point is a panacea. Frankly, I think the boards of these companies are aware of what is going on. When these big questions arise, they go all the way up to Mark Zuckerberg. It is not as if Mark Zuckerberg and the directors of companies such as Meta are unaware of these risks; they are extremely aware of them, as Frances Haugen's testimony made clear.

We do address the governance point. As I say, the risk assessments do need to explain how governance matters are deployed to consider these things—that is in clause 10(6)(h). But for me, it is the sanctions—the powers that Ofcom will have to fine these companies billions of pounds and ultimately to disconnect their service if they do not protect our children—that will deliver the result that we need.

Barbara Keeley: The Minister is talking about companies of such scale that even fines of billions will not hurt them. I refer him to the following wording in the amendments:

"a named individual who the provider considers to be a senior manager of the entity, who may reasonably be expected to be in a position to ensure compliance with the children's risk assessment duties".

That is the minimum we should be asking. We should be asking these platforms, which are doing so much damage and have had to be dragged to the table to do anything at all, to be prepared to appoint somebody who is responsible. The Minister tries to gloss over things by saying, "Oh well, they must be aware of it." The named individual would have to be aware of it. I hope he understands the importance of his role and the Committee's role in making this happen. We could make this happen.

Chris Philp: As I say, clause 10 already references the governance arrangements, but my strong view is that the only thing that will make these companies sit up and take notice—the only thing that will make them actually protect children in a way they are currently not doing—is the threat of billions of pounds of fines and, if they do not comply even after being fined at that level, the threat of their service being disconnected. Ultimately, that is the sanction that will make these companies protect our children.

Kim Leadbeater (Batley and Spen) (Lab): As my hon. Friend the Member for Worsley and Eccles South has said, the point here is about cultural change, and the way to do that is through leadership. It is not about shutting the gate after the horse has bolted. Fining the companies might achieve something, but it does not tackle the root of the problem. It is about cultural change and leadership at these organisations. We all agree across the House that they are not doing enough, so how do we change that culture? It has to come from leadership.

Chris Philp: Yes, and that is why governance is addressed in the clause as drafted. But the one thing that will really change the way the leadership of these companies thinks about this issue is the one thing they ultimately care about—money. The reason they allow unsafe content to circulate and do not rein in or temper their algorithms, and the reason we are in this situation, which has arisen over the last 10 years or so, is that these companies have consistently prioritised profit over protection. Ultimately, that is the only language they understand—it is that and legal compulsion.

While the Bill rightly addresses governance in clause 10 and in other clauses, as I have said a few times, what has to happen to make this change occur is the compulsion that is inherent in the powers to fine and to deny

[Chris Philp]

service—to pull the plug—that the Bill also contains. The thing that will give reassurance to our constituents, and to me as a parent, is knowing that for the first time ever these companies can properly be held to account. They can be fined. They can have their connection pulled out of the wall. Those are the measures that will protect our children.

Alex Davies-Jones: The Minister is being very generous with his time, but I do not think he appreciates the nature of the issue. Mark Zuckerberg's net worth is $71.5 billion. Elon Musk, who is reported to be purchasing Twitter, is worth $218 billion. Bill Gates is worth $125 billion. Money does not matter to these people.

The Minister discusses huge fines for the companies and the potential sanction of bringing down their platforms. They will just set up another one. That is what we are seeing with the smaller platforms: they are closing down and setting up new platforms. These measures do not matter. What matters and will actually make a difference to the safety of children and adults online is personal liability—holding people personally responsible for the direct harm they are causing to people here in the United Kingdom. That is what these amendments seek to do, and that is why we are pushing them so heavily. I urge the Minister to respond to that.

Chris Philp: We discussed personal liability extensively this morning. As we discussed, there is personal liability in relation to providing information, with a criminal penalty of up to two years' imprisonment, to avoid situations like the one we saw a year or two ago, where one of these companies failed to provide the Competition and Markets Authority with the information that it required.

The shadow Minister pointed out the very high levels of global turnover—$71.5 billion—that these companies have. That means that ultimately they can be fined up to $7 billion for each set of breaches. That is a vast amount of money, particularly if those breaches happen repeatedly. She said that such companies will just set up again if we deny their service. Clearly, small companies can close down and set up again the next day, but gigantic companies, such as Meta—Facebook—cannot do that. That is why I think the sanctions I have pointed to are where the teeth really lie.

I accept the point about governance being important as well; I am not dismissing that. That is why we have personal criminal liability for information provision, with up to two years in prison, and it is why governance is referenced in clause 10. I accept the spirit of the points that have been made, but I think the Bill delivers these objectives as drafted.

Dame Maria Miller: Will my hon. Friend give way?

Chris Philp: One last time, because I am conscious that we need to make some progress this afternoon.

Dame Maria Miller: I have huge sympathy with the point that the Minister is making on this issue, but the hon. Member for Pontypridd is right to drive the point home. The Minister says there will be huge fines, but I think there will also be huge court bills. There will be an awful lot of litigation about how things are interpreted, because so much money will come into play. I just reiterate the importance of the guidance and the codes of practice, because if we do not get those right then the whole framework will be incredibly fragile. We will need ongoing scrutiny of how the Bill works or there will be a very difficult situation.

Chris Philp: My right hon. Friend, as always, makes a very good point. The codes of practice will be important, particularly to enable Ofcom to levy fines where appropriate and then successfully defend them. This is an area that may get litigated. I hope that, should lawyers litigating these cases look at our transcripts in the future, they will see how strongly those on both sides of the House feel about this point. I know that Ofcom will ensure that the codes of practice are properly drafted. We touched this morning on the point about timing; we will follow up with Ofcom to make sure that the promise it made us during the evidence session about the road map is followed through and that those get published in good time.

On the point about the Joint Committee, I commend my right hon. Friend for her persistence—*[Interruption.]* Her tenacity—that is the right word. I commend her for her tenacity in raising that point. I mentioned it to the Secretary of State when I saw her at lunchtime, so the point that my right hon. Friend made this morning has been conveyed to the highest levels in the Department.

I must move on to the final two amendments, 11 and 13, which relate to transparency. Again, we had a debate about transparency earlier, when I made the point about the duties in clause 64, which I think cover the issue. Obviously, we are not debating clause 64 now but it is relevant because it requires Ofcom—it is not an option but an obligation; Ofcom must do so—to require providers to produce a transparency report every year. Ofcom can say what is supposed to be in the report, but the relevant schedule lists all the things that can be in it, and covers absolutely everything that the shadow Minister and the hon. Member for Worsley and Eccles South want to see in there.

That requirement to publish transparently and publicly is in the Bill, but it is to be found in clause 64. While I agree with the Opposition's objectives on this point, I respectfully say that those objectives are delivered by the Bill as drafted, so I politely and gently request that the amendments be withdrawn.

Kirsty Blackman: I have a couple of comments, particularly about amendments 15 and 16, which the Minister has just spoken about at some length. I do not agree with the Government's assessment that the governance subsection is adequate. It states that the risk assessment must take into account

"how the design and operation of the service (including the business model, governance, use of proactive technology…may reduce or increase the risks identified."

It is actually an assessment of whether the governance structure has an impact on the risk assessment. It has no impact whatever on the level at which the risk assessment is approved or not approved; it is about the risks that the governance structure poses to children or adults, depending on which section of the Bill we are looking at.

The Minister should consider what is being asked in the amendment, which is about the decision-making level at which the risk assessments are approved. I know the Minister has spoken already, but some clarification would be welcome. Does he expect a junior tech support member of staff, or a junior member of the legal team, to write the risk assessment and then put it in a cupboard? Or perhaps they approve it themselves and then nothing happens with it until Ofcom asks for it. Does he think that Ofcom would look unfavourably on behaviour like that? If he was very clear with us about that, it might put our minds at rest. Does he think that someone in a managerial position or a board member, or the board itself, should take decisions, rather than a very junior member of staff? There is a big spread of people who could be taking decisions. If he could give us an indication of what Ofcom might look favourably on, it would be incredibly helpful for our deliberations.

Chris Philp: I am anxious about time, but I will respond to that point because it is an important one. The hon. Lady is right to say that clause 10(6)(h) looks to identify the risks associated with governance. That is correct—it is a risk assessment. However in clause 11(2)(a), there is a duty to mitigate those risks, having identified what the risks are. If, as she hypothesised, a very junior person was looking at these matters from a governance point of view, that would be identified as a risk. If it was not, Ofcom would find that that was not sufficient or suitable. That would breach clause 10(2), and the service would then be required to mitigate. If it did not mitigate the risks by having a more senior person taking the decision, Ofcom would take enforcement action for its failure under clause 11(2)(a).

For the record, should Ofcom or lawyers consult the transcript to ascertain Parliament's intention in the course of future litigation, it is absolutely the Government's view, as I think it is the hon. Lady's, that a suitable level of decision making for a children's risk assessment would be a very senior level. The official Opposition clearly think that, because they have put it in their amendment. I am happy to confirm that, as a Minister, I think that. Obviously the hon. Lady, who speaks for the SNP, does too. If the transcripts of the Committee's proceedings are examined in the future to ascertain Parliament's intention, Parliament's intention will be very clear.

The Chair: Barbara Keeley, do you have anything to add?

Barbara Keeley: All I have to add is the obvious point—I am sure that we are going to keep running into this—that people should not have to look to a transcript to see what the Minister's and Parliament's intention was. It is clear what the Opposition's intention is—to protect children. I cannot see why the Minister will not specify who in an organisation should be responsible. It should not be a question of ploughing through transcripts of what we have talked about here in Committee; it should be obvious. We have the chance here to do something different and better. The regulator could specify a senior level.

Chris Philp: Clearly, we are legislating here to cover, as I think we said this morning, 25,000 different companies. They all have different organisational structures, different personnel and so on. To anticipate the appropriate level of decision making in each of those companies and put it in the Bill in black and white, in a very prescriptive manner, might not adequately reflect the range of people involved.

3.15 pm

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 10]

AYES

Blackman, Kirsty	Leadbeater, Kim
Carden, Dan	Mishra, Navendu
Davies-Jones, Alex	
Keeley, Barbara	Nicolson, John

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	Stevenson, Jane
Holden, Mr Richard	

Question accordingly negatived.

Barbara Keeley: I beg to move amendment 72, in clause 10, page 9, line 24, after "characteristic" insert "or characteristics".

The Chair: With this it will be convenient to discuss the following:

Amendment 73, in clause 10, page 9, line 24, after "group" insert "or groups".

Amendment 85, in clause 12, page 12, line 22, leave out subsection (d) and insert—

> "(d) the level of risk of harm to adults presented by priority content that is harmful to adults which particularly affects individuals with certain characteristics or members of certain groups;".

This amendment would recognise the intersectionality of harms.

Amendment 74, in clause 12, page 12, line 24, after "characteristic" insert "or characteristics".

Amendment 75, in clause 12, page 12, line 24, after "group" insert "or groups".

Amendment 71, in clause 83, page 72, line 12, at end insert—

> "(1A) For each of the above risks, OFCOM shall identify and assess the level of risk of harm which particularly affects people with certain characteristics or membership of a group or groups."

This amendment requires Ofcom as part of its risk register to assess risks of harm particularly affecting people with certain characteristics or membership of a group or groups.

Barbara Keeley: May I say—this might be a point of order—how my constituency name is pronounced? I get a million different versions, but it is Worsley, as in "worse". It is an unfortunate name for a great place.

I will speak to all the amendments in the group together, because they relate to how levels of risk are assessed in relation to certain characteristics. The amendments are important because small changes to the descriptions of risk assessment will help to close a significant gap in protection.

[Barbara Keeley]

Clauses 10 and 12 introduce a duty on regulated companies to assess harms to adults and children who might have an innate vulnerability arising from being a member of a particular group or having a certain characteristic. However, Ofcom is not required to assess harms to people other than children who have that increased innate vulnerability. Amendment 71 would require Ofcom to assess risks of harm particularly affecting people with certain characteristics or membership of a group or groups as part of its risk register. That would reduce the regulatory burden if companies had Ofcom's risk assessment to base their work on.

Getting this right is important. The risk management regime introduced by the Bill should not assume that all people are at the same risk of harm—they are clearly not. Differences in innate vulnerability increase the incidence and impact of harm, such as by increasing the likelihood of encountering content or of that content being harmful, or heightening the impact of the harm.

It is right that the Bill emphasises the vulnerability of children, but there are other, larger groups with innate vulnerability to online harm. As we know, that often reflects structural inequalities in society.

For example, women will be harmed in circumstances where men might not be, and they could suffer some harms that have a more serious impact than they might for men. A similar point can be made for people with other characteristics. Vulnerability is then compounded by intersectional issues—people might belong to more than one high-risk group—and I will come to that in a moment.

The initial Ofcom risk assessment introduced by clause 83 is not required to consider the heightened risks to different groups of people, but companies are required to assess that risk in their own risk assessments for children and adults. They need to be given direction by an assessment by Ofcom, which amendment 71 would require.

Amendments 72 to 75 address the lack of recognition in these clauses of intersectionality issues. They are small amendments in the spirit of the Bill's risk management regime. As drafted, the Bill refers to a singular "group" or "characteristic" for companies to assess for risk. However, some people are subject to increased risks of harm arising from being members of more than one group. Companies' risk assessments for children and adults should reflect intersectionality, and not just characteristics taken individually. Including the plural of "group" and "characteristic" in appropriate places would achieve that.

Kirsty Blackman: I will first speak to our amendment 85, which, like the Labour amendment, seeks to ensure that the Bill is crystal clear in addressing intersectionality. We need only consider the abuse faced by groups of MPs to understand why that is necessary. Female MPs are attacked online much more regularly than male MPs, and the situation is compounded if they have another minority characteristic. For instance, if they are gay or black, they are even more likely to be attacked. In fact, the MP who is most likely to be attacked is black and female. There are very few black female MPs, so it is not because of sheer numbers that they are at such increased risk of attack. Those with a minority characteristic are at higher risk of online harm, but the risk facing those with more than one minority characteristic is substantially higher, and that is what the amendment seeks to address.

I have spoken specifically about people being attacked on Twitter, Facebook and other social media platforms, but people in certain groups face an additional significant risk. If a young gay woman does not have a community around her, or if a young trans person does not know anybody else who is trans, they are much more likely to use the internet to reach out, to try to find people who are like them, to try to understand. If they are not accepted by their family, school or workplace, they are much more likely to go online to find a community and support—to find what is out there in terms of assistance—but using the internet as a vulnerable, at-risk person puts them at much more significant risk. This goes back to my earlier arguments about people requiring anonymity to protect themselves when using the internet to find their way through a difficult situation in which they have no role models.

It should not be difficult for the Government to accept this amendment. They should consider it carefully and understand that all of us on the Opposition Benches are making a really reasonable proposal. This is not about saying that someone with only one protected characteristic is not at risk; it is about recognising the intersectionality of risk and the fact that the risk faced by those who fit into more than one minority group is much higher than that faced by those who fit into just one. This is not about taking anything away from the Bill; it is about strengthening it and ensuring that organisations listen.

We have heard that a number of companies are not providing the protection that Members across the House would like them to provide against child sexual abuse. The governing structures, risk assessments, rules and moderation at those sites are better at ensuring that the providers make money than they are at providing protection. When regulated providers assess risk, it is not too much to ask them to consider not just people with one protected characteristic but those with multiple protected characteristics.

As MPs, we work on that basis every day. Across Scotland and the UK, we support our constituents as individuals and as groups. When protected characteristics intersect, we find ourselves standing in Parliament, shouting strongly on behalf of those affected and giving them our strongest backing, because we know that that intersection of harms is the point at which people are most vulnerable, in both the real and the online world. Will the Minister consider widening the provision so that it takes intersectionality into account and not only covers people with one protected characteristic but includes an over and above duty? I genuinely do not think it is too much for us to ask providers, particularly the biggest ones, to make this change.

Chris Philp: Once again, the Government recognise the intent behind these amendments and support the concept that people with multiple intersecting characteristics, or those who are members of multiple groups, may experience—or probably do experience—elevated levels of harm and abuse online compared with others. We completely understand and accept that point, as clearly laid out by the hon. Member for Aberdeen North.

There is a technical legal reason why the use of the singular characteristic and group singular is adopted here. Section 6(c) of the Interpretation Act 1978 sets out how words in Bills and Acts are interpreted, namely that such words in the singular also cover the plural. That means that references in the singular, such as

"individuals with a certain characteristic"

in clause 10(6)(d), also cover characteristics in the plural. A reference to the singular implies a reference to the plural.

Will those compounded risks, where they exist, be taken into account? The answer is yes, because the assessments must assess the risk in front of them. Where there is evidence that multiple protected characteristics or the membership of multiple groups produce compounded risks, as the hon. Lady set out, the risk assessment has to reflect that. That includes the general sectoral risk assessment carried out by Ofcom, which is detailed in clause 83, and Ofcom will then produce guidance under clause 84.

The critical point is that, because there is evidence of high levels of compounded risk when people have more than one characteristic, that must be reflected in the risk assessment, otherwise it is inadequate. I accept the point behind the amendments, but I hope that that explains, with particular reference to the 1978 Act, why the Bill as drafted covers that valid point.

The Chair: Barbara Keeley?

Barbara Keeley: I have nothing to add. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 10 ordered to stand part of the Bill.

Clause 11

Safety duties protecting children

The Chair: We now come to amendment 95, tabled by the hon. Member for Upper Bann, who is not on the Committee. Does anyone wish to move the amendment? If not, we will move on.

Barbara Keeley: I beg to move amendment 29, in clause 11, page 10, line 20, at end insert—

"(c) prevent the sexual or physical abuse of a child by means of that service."

This amendment establishes a duty to prevent the sexual or physical abuse of a child by means of a service.

The Chair: With this it will be convenient to discuss amendment 33, in clause 26, page 26, line 18, at end insert—

"(c) prevent the sexual or physical abuse of a child by means of that service."

This amendment establishes a duty to prevent the sexual or physical abuse of a child by means of a service.

3.30 pm

Barbara Keeley: The purpose of this clause is to ensure that children at risk of online harms are given protections from harmful, age-inappropriate content through specific children's safety duties for user-to-user services likely to be accessed by children.

It is welcome that the Bill contains strong provisions to ensure that service providers act upon and mitigate the risks identified in the required risk assessment, and to introduce protective systems and processes to address what children encounter. This amendment aims to ensure that online platforms are proactive in their attempts to mitigate the opportunity for sex offenders to abuse children.

As we have argued with other amendments, there are missed opportunities in the Bill to be preventive in tackling the harm that is created. The sad reality is that online platforms create an opportunity for offenders to identify, contact and abuse children, and to do so in real time through livestreaming. We know there has been a significant increase in online sexual exploitation during the pandemic. With sex offenders unable to travel or have physical contact with children, online abuse increased significantly.

In 2021, UK law enforcement received a record 97,727 industry reports relating to online child abuse, a 29% increase on the previous year, which is shocking. An NSPCC freedom of information request to police forces in England and Wales last year showed that online grooming offences reached record levels in 2020-21, with the number of sexual communications with a child offences in England and Wales increasing by almost 70% in three years. There has been a deeply troubling trend in internet-facilitated abuse towards more serious sexual offences against children, and the average age of children in child abuse images, particularly girls, is trending to younger ages.

In-person contact abuse moved online because of the opportunity there for sex offenders to continue exploiting children. Sadly, they can do so with little fear of the consequences, because detection and disruption of livestreamed abuse is so low. The duty to protect children from sexual offenders abusing them in real time and livestreaming their exploitation cannot be limited to one part of the internet and tech sector. While much of the abuse might take place on the user-to-user services, it is vital that protections against such abuse are strengthened across the board, including in the search services, as set out in clause 26.

At the moment there is no list of harms in the Bill that must be prioritised by regulated companies. The NSPCC and others have suggested including a new schedule, similar to schedule 7, setting out what the primary priority harms should be. It would be beneficial for the purposes of parliamentary scrutiny for us to consider the types of priority harm that the Government intend the Bill to cover, rather than leaving that to secondary legislation. I hope the Minister will consider that and say why it has not yet been included.

To conclude, while we all hope the Bill will tackle the appalling abuse of children currently taking place online, this cannot be achieved without tackling the conditions in which these harms can take place. It is only by requiring that steps be taken across online platforms to limit the opportunities for sex offenders to abuse children that we can see the prevalence of this crime reduced.

Dame Maria Miller: I rise, hopefully to speak to clause 11 more generally—or will that be a separate stand part debate, Ms Rees?

The Chair: That is a separate debate.

Dame Maria Miller: My apologies. I will rise later.

Chris Philp: The Government obviously support the objective of these amendments, which is to prevent children from suffering the appalling sexual and physical abuse that the hon. Member for Worsley and Eccles South outlined in her powerful speech. It is shocking that these incidents have risen in the way that she described.

To be clear, that sort of appalling sexual abuse is covered in clause 9—which we have debated already—which covers illegal content. As Members would expect, child sexual abuse is defined as one of the items of priority illegal content, which are listed in more detail in schedule 6, where the offences that relate to sexual abuse are enumerated. As child sexual exploitation is a priority offence, services are already obliged through clause 9 to be "proactive" in preventing it from happening. As such, as Members would expect, the requirements contained in these amendments are already delivered through clause 9.

The hon. Member for Worsley and Eccles South also asked when we are going to hear what the primary priority harms to children might be. To be clear, those will not include the sexual exploitation offences, because as Members would also expect, those are already in the Bill as primary illegal offences. The primary priority harms might include material promoting eating disorders and that kind of thing, which is not covered by the criminal matters—the illegal matters. I have heard the hon. Lady's point that if that list were to be published, or at least a draft list, that would assist Parliament in scrutinising the Bill. I will take that point away and see whether there is anything we can do in that area. I am not making a commitment; I am just registering that I have heard the point and will take it away.

Barbara Keeley: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Question proposed, That the clause stand part of the Bill.

The Chair: With this it will be convenient to discuss clause 26 stand part.

Dame Maria Miller: I rise to speak to clause 11, because this is an important part of the Bill that deals with the safety duties protecting children. Many of us here today are spurred on by our horror at the way in which internet providers, platform providers and search engines have acted over recent years, developing their products with no regard for the safety of children, so I applaud the Government for bringing forward this groundbreaking legislation. They are literally writing the book on this, but in doing so, we have be very careful about the language we use and the way in which we frame our requirements of these organisations. The Minister has rightly characterised these organisations as being entirely driven by finance, not the welfare of their consumers, which must make them quite unique in the world. I can only hope that that will change: presumably, over time, people will not want to use products that have no regard for the safety of those who use them.

In this particular part of the Bill, the thorny issue of age assurance comes up. I would value the Minister's views on some of the evidence that we received during our evidence sessions about how we ensure that age assurance is effective. Some of us who have been in this place for a while would be forgiven for thinking that we had already passed a law on age assurance. Unfortunately, that law did not seem to come to anything, so let us hope that second time is lucky. The key question is: who is going to make sure that the age assurance that is in place is good enough? Clause 11(3) sets out

"a duty to operate a service using proportionate systems and processes"

that is designed to protect children, but what is a proportionate system? Who is going to judge that? Presumably it will be Ofcom in the short term, and in the long term, I am sure the courts will get involved.

In our evidence, we heard some people advocating very strongly for these sorts of systems to be provided by third parties. I have to say, in a context where we are hearing how irresponsible the providers of these services are, I can understand why people would think that a third party would be a more responsible way forward. Can the Minister help the Committee understand how Ofcom will ensure that the systems used, particularly the age assurance systems, are proportionate—I do not particularly like that word; I would like those systems to be brilliant, not proportionate—and are actually doing what we need them to do, which is safeguard children? For the record, and for the edification of judges who are looking at this matter in future—and, indeed, Ofcom—will he set out how important this measure is within the Bill?

Chris Philp: I thank my right hon. Friend for her remarks, in which she powerfully and eloquently set out how important the clause is to protecting children. She is right to point out that this is a critical area in the Bill, and it has wide support across the House. I am happy to emphasise, for the benefit of those who may study our proceedings in future, that protecting children is probably the single-most important thing that the Bill does, which is why it is vital that age-gating, where necessary, is effective.

My right hon. Friend asked how Ofcom will judge whether the systems under clause 11(3) are proportionate to

"prevent children of any age from encountering"

harmful content and so on. Ultimately, the proof of the pudding is in the eating; it has to be effective. When Ofcom decides whether a particular company or service is meeting the duty set out in the clause, the simple test will be one of effectiveness: is it effective and does it work? That is the approach that I would expect Ofcom to take; that is the approach that I would expect a court to take. We have specified that age verification, which is the most hard-edged type of age assurance—people have to provide a passport or something of that nature—is one example of how the duty can be met. If another, less-intrusive means is used, it will still have to be assessed as effective by Ofcom and, if challenged, by the courts.

I think my right hon. Friend was asking the Committee to confirm to people looking at our proceedings our clear intent for the measures to be effective. That is the standard to which we expect Ofcom and the courts to hold those platforms in deciding whether they have met the duties set out in the clause.

Dame Maria Miller: For clarification, does the Minister anticipate that Ofcom might be able to insist that a third-party provider be involved if there is significant evidence that the measures put in place by a platform are ineffective?

Chris Philp: We have deliberately avoided being too prescriptive about precisely how the duty is met. We have pointed to age verification as an example of how the duty can be met without saying that that is the only way. We would not want to bind Ofcom's hands, or indeed the hands of platforms. Clearly, using a third party is another way of delivering the outcome. If a platform were unable to demonstrate to Ofcom that it could deliver the required outcome using its own methods, Ofcom may well tell it to use a third party instead. The critical point is that the outcome must be delivered. That is the message that the social media firms, Ofcom and the courts need to hear when they look at our proceedings. That is set out clearly in the clause. Parliament is imposing a duty, and we expect all those to whom the legislation applies to comply with it.

Question put and agreed to.

Clause 11 accordingly ordered to stand part of the Bill.

Clause 12

ADULTS' RISK ASSESSMENT DUTIES

Alex Davies-Jones: I beg to move amendment 12, in clause 12, page 12, line 10, at end insert—

"(4A) A duty to publish the adults' risk assessment and proactively supply this to OFCOM."

This amendment creates a duty to publish the adults' risk assessment and supply it to Ofcom.

The Chair: With this it will be convenient to discuss clause stand part.

Alex Davies-Jones: The amendment creates a duty to publish the adults' risk assessment and supply it to Ofcom. As my hon. Friend the Member for Worsley and Eccles South remarked when addressing clause 10, transparency and scrutiny of those all-important risk assessments must be at the heart of the Online Safety Bill. We all know that the Government have had a hazy record on transparency lately but, for the sake of all in the online space, I sincerely hope that the Minister will see the value in ensuring that the risk assessments are accurate, proactively supplied and published for us all to consider.

It is only fair that all the information about risks to personal safety be made available to users of category 1 services, which we know are the most popular and, often, the most troublesome services. We all want people to feel compelled to make their own decisions about their behaviour both online and offline. That is why we are pushing for a thorough approach to risk assessments more widely. Also, without a formal duty to publicise those risk assessments, I fear there will be little change in our safety online. The Minister has referenced that the platforms will be looking back at *Hansard* in years to come to determine whether or not they should be doing the right thing. Unless we make that a statutory obligation within the Bill, I fear that reference will fall on deaf ears.

3.45 pm

The Government have made some positive steps towards keeping children safe online. Sadly, the same cannot be said for adults. We need to be careful when we formally differentiate between children and adults, because age, as they say, is but only a number. A 17-year-old will obviously fall short of being legally deemed an adult in this country, but an 18-year-old, who only a few months or even a day earlier was 17, should have exactly the same protections. Platforms should of course be required to protect adults too.

We have seen what years of no accountability has done to the online space. My hon. Friend referred to Frances Haugen's experiences at Meta, which we all heard about recently in evidence sessions—none of it filled me with confidence. We know that those category 1 companies have the information, but they will not feel compelled to publish it until there is a statutory duty to do so. The Minister knows that would be an extremely welcome move; he would be commended by academics, stakeholders, parliamentarians and the public alike. Why exactly does that glaring omission still remain? If the Minister cannot answer me fully, and instead refers to platforms looking to *Hansard* in the future, then I am keen to press this amendment to a Division. I cannot see the benefits of withholding those risk assessments from the public and academics.

Chris Philp: Once again, I agree with the point about transparency and the need to have those matters brought into the light of day. We heard from Frances Haugen how Facebook—now Meta—actively resisted doing so. However, I point to two provisions already in the Bill that deliver precisely that objective. I know we are debating clause 12, but there is a duty in clause 13(2) for platforms to publish in their terms of service—a public document—the findings of the most recent adult risk assessment. That duty is in clause 13—the next clause we are going to debate—in addition to the obligations I have referred to twice already in clause 64, where Ofcom compels those firms to publish their transparency reports. I agree with the points that the shadow Minister made, but suggest that through clause 13(2) and clause 64, those objectives are met in the Bill as drafted.

Alex Davies-Jones: I thank the Minister for his comments, but sadly we do not feel that is appropriate or robust enough, which is why we will be pressing the amendment to a Division.

Question put, That the amendment be made.

The Committee divided.

The Committee divided: Ayes 5, Noes 9.

Division No. 11]

AYES

Carden, Dan	Leadbeater, Kim
Davies-Jones, Alex	
Keeley, Barbara	Mishra, Navendu

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	Stevenson, Jane
Holden, Mr Richard	

Question accordingly negatived.

Clause 12 ordered to stand part of the Bill.

Clause 13

SAFETY DUTIES PROTECTING ADULTS

Question proposed, That the clause stand part of the Bill.

Alex Davies-Jones: While I am at risk of parroting my hon. Friend the Member for Worsley and Eccles South on clause 11, it is important that adults and the specific risks they face online are considered in the clause. The Minister knows we have wider concerns about the specific challenges of the current categorisation system. I will come on to that at great length later, but I thought it would be helpful to remind him at this relatively early stage that the commitments to safety and risk assessments for category 1 services will only work if category 1 encapsulates the most harmful platforms out there. That being said, Labour broadly supports this clause and has not sought to amend it.

Chris Philp: I am eagerly awaiting the lengthy representations that the shadow Minister just referred to, as are, I am sure, the whole Committee and indeed the millions watching our proceedings on the live broadcast. As the shadow Minister said, clause 13 sets out the safety duties in relation to adults. This is content that is legal but potentially harmful to adults, and for those topics specified in secondary legislation, it will require category 1 services to set out clearly what actions they might be taking—from the actions specified in subsection (4) —in relation to that content.

It is important to specify that the action they may choose to take is a choice for the platform. I know some people have raised issues concerning free speech and these duties, but I want to reiterate and be clear that this is a choice for the platform. They have to be publicly clear about what choices they are making, and they must apply those choices consistently. That is a significant improvement on where we are now, where some of these policies get applied in a manner that is arbitrary.

Question put and agreed to.

Clause 13 accordingly ordered to stand part of the Bill.

Clause 14

USER EMPOWERMENT DUTIES

Alex Davies-Jones: I beg to move amendment 46, in clause 14, page 14, line 12, after "non-verified users" insert

"and to enable them to see whether another user is verified or non-verified."

This amendment would make it clear that, as part of the User Empowerment Duty, users should be able to see which other users are verified and which are non-verified.

The Chair: With this it will be convenient to discuss the following:

Amendment 47, in clause 189, page 155, line 1, at end insert

> "'Identity Verification' means a system or process designed to enable a user to prove their identity, for purposes of establishing that they are a genuine, unique, human user of the service and that the name associated with their profile is their real name."

This amendment adds a definition of Identity Verification to the terms defined in the Bill.

New clause 8—*OFCOM's guidance about user identity verification*—

"(1) OFCOM must produce guidance for providers of Category 1 services on how to comply with the duty set out in section 57(1).

(2) In producing the guidance (including revised or replacement guidance), OFCOM must have regard to—

(a) ensuring providers offer forms of identity verification which are likely to be accessible to vulnerable adult users and users with protected Characteristics under the Equality Act 2010,

(b) promoting competition, user choice, and interoperability in the provision of identity verification,

(c) protection of rights, including rights to privacy, freedom of expression, safety, access to information, and the rights of children,

(d) alignment with other relevant guidance and regulation, including with regards to Age Assurance and Age Verification.

(3) In producing the guidance (including revised or replacement guidance), OFCOM must set minimum standards for the forms of identity verification which Category services must offer, addressing—

(a) effectiveness,

(b) privacy and security,

(c) accessibility,

(d) time-frames for disclosure to Law Enforcement in case of criminal investigations,

(e) transparency for the purposes of research and independent auditing,

(f) user appeal and redress mechanisms.

(4) Before producing the guidance (including revised or replacement guidance), OFCOM must consult—

(a) the Information Commissioner,

(b) the Digital Markets Unit,

(c) persons whom OFCOM consider to have technological expertise relevant to the duty set out in section 57(1),

(d) persons who appear to OFCOM to represent the interests of users including vulnerable adult users of Category 1 services, and

(e) such other persons as OFCOM considers appropriate.

(5) OFCOM must publish the guidance (and any revised or replacement guidance)."

This new clause would require Ofcom to set a framework of principles and minimum standards for the User Verification Duty.

Alex Davies-Jones: The revised Bill seeks to address the problems associated with anonymity through requiring platforms to empower users, with new options to verify their identity and filter out non-verified accounts. This is in line with the approach recommended by Clean Up The Internet and also reflects the approach proposed in the Social Media Platforms (Identity Verification) Bill, which was tabled by the hon. Member for Stroud (Siobhan Baillie) and attracted cross-party support. It has the potential to strike a better balance between tackling the clear role that anonymity can play in fuelling abuse and disinformation, while safeguarding legitimate uses of anonymity, including by vulnerable users, for whom anonymity can act as a protection. However, Labour does share the concerns of stakeholders around the revised Bill, which we have sought to amend.

Amendment 46 aims to empower people to use this information about verification when making judgments about the reliability of other accounts and the content

they share. This would ensure that the user verification duty helps disrupt the use of networks of inauthentic accounts to spread disinformation. Labour welcomes the inclusion in the revised Bill of measures designed to address harm associated with misuse of anonymous social media accounts. There is considerable evidence from Clean Up The Internet and others that anonymity fuels online abuse, bullying and trolling and that it is one of the main tools used by organised disinformation networks to spread and amplify false, extremist and hateful content.

The revised Bill seeks to address the problems associated with anonymity, by requiring platforms to empower users with new options to verify their identity and to filter out non-verified accounts. In doing so, it has the potential to strike a better balance between tackling the clear role that anonymity can play in fuelling abuse and misinformation while safeguarding legitimate users of anonymity, including vulnerable users, for whom anonymity acts as a protection.

Clause 14 falls short of truly empowering people to make the most well-informed decisions about the type of content they engage with. We believe that this could be simple, and a simple change from a design perspective. Category 1 platforms are already able to verify different types of accounts, whether they be personal or business accounts, so ensuring that people are equipped with this information more broadly would be an easy step for the big platforms to make. Indeed, the Joint Committee's prelegislative scrutiny recommended that the Government consider, as part of Ofcom's code of practice, a requirement for the largest and highest-risk platforms to offer the choice of verified or unverified status and user options on how they interact with accounts in either category.

I know that there are concerns about verification, and there is a delicate balance between anonymity, free speech and protecting us all online. I somewhat sympathise with the Minister in being tasked with bringing forward this complex legislation, but the options for choosing what content and users we do and do not engage with are already there on most platforms. On Twitter, we are able to mute accounts—I do so regularly—or keywords that we want to avoid. Similarly, we can restrict individuals on Instagram.

In evidence to the Joint Committee, the Secretary of State said that the first priority of the draft Bill was to end all online abuse, not just that from anonymous accounts. Hopes were raised about the idea of giving people the option to limit their interaction with anonymous or non-verified accounts. Clearly, the will is there, and the amendment ensures that there is a way, too. I urge the Minister to accept the amendment, if he is serious about empowering users across the United Kingdom.

Now I move on to amendment 47. As it stands, the Bill does not adequately define "verification" or set minimum standards for how it will be carried out. There is a risk that platforms will treat this as a loophole in order to claim that their current, wholly inadequate processes count as verification. We also see entirely avoidable risks of platforms developing new verification processes that fail to protect users' privacy and security or which serve merely to extend their market dominance to the detriment of independent providers. That is why it is vital that a statutory definition of identity verification is placed in the Bill.

I have already spoken at length today, and I appreciate that we are going somewhat slowly on the Bill, but it is complex legislation and this is an incredibly important detail that we need to get right if the Bill is to be truly world leading. Without a definition of identity verification, I fear that we are at risk of allowing technology, which can easily replicate the behaviours of a human being, to run rife, which would essentially invalidate the process of verification entirely.

I have also spoken at length about my concerns relating to AI technologies, the lack of future proofing in the Bill and the concerns that could arise in the future. I am sure that the Minister is aware that that could have devastating impacts on our democracy and our online safety more widely.

New clause 8 would ensure that the user empowerment duty and user verification work as intended by simply requiring Ofcom to set out principles and minimum standards for compliance. We note that the new clause is entirely compatible with the Government's stated aims for the Bill and would provide a clearer framework for both regulated companies and the regulator. By its very nature, it is vital that in preparing the guidance Ofcom must ensure that the delicate balance that I touched on earlier between freedom of expression, the right to privacy and safety online is kept in mind throughout.

We also felt it important that, in drawing up the guidance a collaborative approach should be taken. Regulating the online space is a mammoth task, and while we have concerns about Ofcom's independence, which I will gladly touch on later, we also know that it will be best for us all if it is required to draw on the expertise of other expert organisations in doing so.

The Chair: There is a Division in the House, so I will suspend the sitting for 15 minutes.

3.58 pm

Sitting suspended for a Division in the House.

4.13 pm

On resuming—

The Chair: If no other Member would like to speak to amendment 46, I call the Minister.

Chris Philp: I would be delighted to speak to the amendment, which would change the existing user empowerment duty in clause 14 to require category 1 services to enable adult users to see whether other users are verified. In effect, however, that objective already follows as a natural consequence of the duty in clause 14(6). When a user decides to filter out non-verified users, by definition such users will be able to see content only from verified users, so they could see from that who was verified and who was not. The effect intended by the amendment, therefore, is already achieved through clause 14(6).

Kirsty Blackman: I am sorry to disagree with the Minister so vigorously, but that is a rubbish argument. It does not make any sense. There is a difference between wanting to filter out everybody who is not verified and wanting to actually see if someone who is threatening

[Kirsty Blackman]

someone else online is a verified or a non-verified user. Those are two very different things. I can understand why a politician, for example, might not want to filter out unverified users but would want to check whether a person was verified before going to the police to report a threat.

Chris Philp: When it comes to police investigations, if something is illegal and merits a report to the police, users should report it, regardless of whether someone is verified or not—whatever the circumstances. I would encourage any internet user to do that. That effectively applies on Twitter already; some people have blue ticks and some people do not, and people should report others to the police if they do something illegal, whether or not they happen to have a blue tick.

Amendment 47 seeks to create a definition of identity verification in clause 189. In addition, it would compel the person's real name to be displayed. I understand the spirit of the amendment, but there are two reasons why I would not want to accept it and would ask hon. Members not to press it. First, the words "identity verification" are ordinary English words with a clear meaning and we do not normally define in legislation ordinary English words with a clear meaning. Secondly, the amendment would add the new requirement that, if somebody is verified, their real name has to be displayed, but I do not think that that is the effect of the drafting as it stands. Somebody may be verified, and the company knows who they are—if the police go to the company, they will have the verified information—but there is no obligation, as the amendment is drafted, for that information to be displayed publicly. The effect of that part of the amendment would be to force users to choose between disclosing their identity to everyone or having no control over who they interact with. That may not have been the intention, but I am not sure that this would necessarily make sense.

New clause 8 would place requirements on Ofcom about how to produce guidance on user identity verification and what that guidance must contain. We already have provisions on that in clause 58, which we will no doubt come to, although probably not later on today—maybe on Thursday. Clause 58 allows Ofcom to include in its regulatory guidance the principles and standards referenced in the new clause, which can then assist service providers in complying with their duties. Of course, if they choose to ignore the guidelines and do not comply with their duties, they will be subject to enforcement action, but we want to ensure that there is flexibility for Ofcom, in writing those guidelines, and for companies, in following those guidelines or taking alternative steps to meet their duty.

This morning, a couple of Members talked about the importance of remaining flexible and being open to future changes in technology and a wide range of user needs. We want to make sure that flexibility is retained. As drafted, new clause 8 potentially undermines that flexibility. We think that the powers set out in clause 58 give Ofcom the ability to set the relevant regulatory guidance.

Clause 14 implements the proposals made by my hon. Friend the Member for Stroud in her ten-minute rule Bill and the proposals made, as the shadow Minister has said, by a number of third-party stakeholders. We should all welcome the fact that these new user empowerment duties have now been included in the Bill in response to such widespread parliamentary lobbying.

Alex Davies-Jones: I am grateful to the Minister for giving way. I want to recount my own experience on this issue. He mentioned that anybody in receipt of anonymous abuse on social media should report it to the police, especially if it is illegal. On Thursday, I dared to tweet my opinions on the controversial Depp-Heard case in America. As a result of putting my head above the parapet, my Twitter mentions were an absolute sewer of rape threats and death threats, mainly from anonymous accounts. My Twitter profile was mocked up—I had devil horns and a Star of David on my forehead. It was vile. I blocked, deleted and moved on, but I also reported those accounts to Twitter, especially those that sent me rape threats and death threats.

That was on Thursday, and to date no action has been taken and I have not received any response from Twitter about any of the accounts I reported. The Minister said they should be reported to the police. If I reported all those accounts to the police, I would still be there now reporting them. How does he anticipate that this will be resourced so that social media companies can tackle the issue? That was the interaction resulting from just one tweet that I sent on Thursday, and anonymous accounts sent me a barrage of hate and illegal activity.

Chris Philp: The shadow Minister raises a very good point. Of course, what she experienced on Twitter was despicable, and I am sure that all members of the Committee would unreservedly condemn the perpetrators who put that content on there. Once the Bill is passed, there will be legal duties on Twitter to remove illegal content. At the moment, they do not exist, and there is no legal obligation for Twitter to remove that content, even though much of it, from the sound of it, would cross one of various legal thresholds. Perhaps some messages qualify as malicious communication, and others might cross other criminal thresholds. That legal duty does not exist at the moment, but when this Bill passes, for the first time there will be that duty to protect not just the shadow Minister but users across the whole country.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 8.

Division No. 12]

AYES

Blackman, Kirsty	Keeley, Barbara
Carden, Dan	Leadbeater, Kim
Davies-Jones, Alex	Mishra, Navendu

NOES

Ansell, Caroline	Holden, Mr Richard
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	Stevenson, Jane

Question accordingly negatived.

Clause 14 ordered to stand part of the Bill.

Clause 15

DUTIES TO PROTECT CONTENT OF DEMOCRATIC IMPORTANCE

Kim Leadbeater: I beg to move amendment 105, in clause 15, page 14, line 33, after "ensure" insert "the safety of people involved in UK elections and".

The Chair: With this it will be convenient to discuss amendment 106, in clause 37, page 25, line 31, at end insert—

'(2A) OFCOM must prepare and issue a code of practice for providers of Category 1 and 2(a) services describing measures recommended for the purpose of compliance with duties set out in section 15 concerning the safety of people taking part in elections."

Kim Leadbeater: I rise to speak to amendments 105 and 106, in my name, on protecting democracy and democratic debate.

Within the Bill, there are significant clauses intended to prevent the spread of harm online, to protect women and girls against violence and to help prevent child sexual exploitation, while at the same time protecting the right of journalists to do their jobs. Although those clauses are not perfect, I welcome them.

The Bill is wide-ranging. The Minister talked on Second Reading about the power in clause 150 to protect another group—those with epilepsy—from being trolled with flashing images. That subject is close to my heart due to the campaign for Zach's law—Zach is a young boy in my constituency. I know we will return to that important issue later in the Committee, and I thank the Minister for his work on it.

In protecting against online harm while preserving fundamental rights and values, we must also address the threats posed to those involved in the democratic process. Let me be clear: this is not self-serving. It is about not just MPs but all political candidates locally and nationally and those whose jobs facilitate the execution of our democratic process and political life: the people working on elections or for those elected to public office at all levels across the UK. These people must be defended from harm not only for their own protection, but to protect our democracy itself and, with it, the right of all our citizens to a political system capable of delivering on their priorities free from threats and intimidation.

Many other groups in society are also subjected to a disproportionate amount of targeted abuse, but those working in and around politics sadly receive more than almost any other people in this country, with an associated specific set of risks and harms. That does not mean messages gently, or even firmly, requesting us to vote one way or another—a staple of democratic debate—but messages of hate, abuse and threats intended to scare people in public office, grind them down, unfairly influence their voting intentions or do them physical and psychological harm. That simply cannot be an acceptable part of political life.

As I say, we are not looking for sympathy, but we have a duty to our democracy to try to stamp that out from our political discourse. Amendment 105 would not deny anybody the right to tell us firmly where we are going wrong—quite right, too—but it is an opportunity to draw the essential distinction between legitimately holding people in public life to account and illegitimate intimidation and harm.

The statistics regarding the scale of online abuse that MPs receive are shocking. In 2020, a University of Salford study found that MPs received over 7,000 abusive or hate-filled tweets a month. Seven thousand separate messages of harm a month on Twitter alone directed at MPs is far too many, but who in this room does not believe that the figure is almost certainly much higher today? Amnesty conducted a separate study in 2017 looking at the disproportionate amount of abuse that women and BAME MPs faced online, finding that my right hon. Friend the Member for Hackney North and Stoke Newington (Ms Abbott) was the recipient of almost a third of all the abusive tweets analysed, as alluded to already by the hon. Member for Edinburgh—

Kirsty Blackman: Aberdeen North.

Kim Leadbeater: I knew that. *[Laughter.]*

Five years later, we continue to see significant volumes of racist, sexist and homophobic hate-filled abuse and threats online to politicians of all parties. That is unacceptable in itself, but we must ask whether this toxic environment helps to keep decent people in politics or, indeed, attracts good people into politics, so that our democracy can prosper into the future across the political spectrum. The reality we face is that our democracy is under attack online each and every day, and every day we delay acting is another day on which abuse becomes increasingly normalised or is just seen as part of the job for those who have put themselves forward for public service. This form of abuse harms society as a whole, so it deserves specific consideration in the Bill.

While elected Members and officials are not a special group of people deserving of more legal protections than anyone else, we must be honest that the abuse they face is distinct and specific to those roles and directly affects our democracy itself. It can lead to the most serious physical harm, with two Members of Parliament having been murdered in the last six years, and many others face death threats or threats of sexual or other violence on a daily basis. However, this is not just about harm to elected representatives; online threats are often seen first, and sometimes only, by their members of staff. They may not be the intended target, but they are often the people harmed most. I am sure we all agree that that is unacceptable and cannot continue.

All of us have probably reported messages and threats to social media platforms and the police, with varying degrees of success in terms of having them removed or the individuals prosecuted. Indeed, we sadly heard examples of that from my hon. Friend the shadow Minister. Often we are told that nothing can be done. Currently, the platforms look at their own rules to determine what constitutes freedom of speech or expression and what is hateful speech or harm. That fine line moves. There is no consistency across platforms, and we therefore urgently need more clarity and a legal duty in place to remove that content quickly.

Amendment 105 would explicitly include in the Bill protection and consideration for those involved in UK elections, whether candidates or staff. Amendment 106 would go further and place an obligation on Ofcom to produce a code of practice, to be issued to the platforms. It would define what steps platforms must take to

[Kim Leadbeater]

protect those involved in elections and set out what content is acceptable or unacceptable to be directed at them.

4.30 pm

While I am cautious about heaping responsibility on Ofcom and I remain nervous about the Government's willingness to leave more and more contentious issues for it to deal with, I believe that that is a reasonable step. It would allow Ofcom to outline what steps a platform must take to protect democratic debate and to set out acceptable and unacceptable content in the context of our ever-changing political landscape. That form of nuance would need to be regularly updated, so it clearly would not be practical to put it in the Bill.

Let us be honest: will this amendment solve the issue entirely? No. However, does more need to be done to protect our democracy? Yes. I am in constant conversation with people and organisations in this sector about what else could be brought forward to assist the police and the Crown Prosecution Service in prosecuting those who wish to harm those elected to public office—both online and offline. Directly addressing the duty of platforms to review content, remove harmful speech and report those who wish to do harm would, I believe, be a positive first step towards protecting our democratic debate and defending those who work to make it effective on behalf of the people of the United Kingdom.

Kirsty Blackman: I want to make a few comments on the amendment. As a younger female parliamentarian, I find that I am often asked to speak to young people about becoming an MP or getting involved in politics. I find it difficult to say to young women, "Yes, you should do this," and most of the reason for that is what people are faced with online. It is because a female MP cannot have a Twitter account without facing abuse. I am sure male MPs do as well, but it tends to be worse for women.

We cannot engage democratically and with constituents on social media platforms without receiving abuse and sometimes threats as well. It is not just an abusive place to be—that does not necessarily meet the threshold for illegality—but it is pretty foul and toxic. There have been times when I have deleted Twitter from my phone because I just need to get away from the vile abuse that is being directed towards me. I want, in good conscience, to be able to make an argument to people that this is a brilliant job, and it is brilliant to represent constituents and to make a difference on their behalf at whatever level of elected politics, but right now I do not feel that I am able to do that.

When my footballing colleague, the hon. Member for Batley and Spen, mentions "UK elections" in the amendment, I assume she means that in the widest possible way—elections at all levels.

Kim Leadbeater *indicated assent.*

Kirsty Blackman: Sometimes we miss out the fact that although MPs face abuse, we have a level of protection as currently elected Members. Even if there were an election coming up, we have a level of security protection and access that is much higher than for anybody else challenging a candidate or standing in a council or a Scottish Parliament election. As sitting MPs, we already have an additional level of protection because of the security services we have in place. We need to remember, and I assume this is why the amendment is drawn in a pretty broad way, that everybody standing for any sort of elected office faces significant risk of harm—again, whether or not that meets the threshold for illegality.

There are specific things that have been mentioned. As has been said, epilepsy is specifically mentioned as a place where specific harm occurs. Given the importance of democracy, which is absolutely vital, we need to have a democratic system where people are able to stand in elections and make their case. Given the importance of democracy, which is absolutely vital, we need to have a democratic system where people are able to stand in elections and make their case. That is why we have election addresses and a system where the election address gets delivered through every single person's door. There is an understanding and acceptance by people involved in designing democratic processes that the message of all candidates needs to get out there. If the message of all candidates cannot get out there because some people are facing significant levels of abuse online, then democracy is not acting in the way that it should be. These amendments are fair and make a huge amount of sense. They are protecting the most important tenets of democracy and democratic engagement.

I want to say something about my own specific experiences. We have reported people to the police and have had people in court over the messages they have sent, largely by email, which would not be included in the Bill, but there have also been some pretty creepy ones on social media that have not necessarily met the threshold. As has been said, it is my staff who have had to go to court and stand in the witness box to explain the shock and terror they have felt on seeing the email or the communication that has come in, so I think any provision should include that.

Finally, we have seen situations where people working in elections—this is not an airy-fairy notion, but something that genuinely happened—have been photographed and those pictures have been shared on social media, and they have then been abused as a result. They are just doing their job, handing out ballot papers or standing up and announcing the results on the stage, and they have to abide by the processes that are in place now. In order for us to have free and fair elections that are run properly and that people want to work at and support, we need to have that additional level of protection. The hon. Member for Batley and Spen made a very reasonable argument and I hope the Minister listened to it carefully.

Chris Philp: I have listened very carefully to both the hon. Member for Batley and Spen and the hon. Member for Aberdeen North. I agree with both of them that abuse and illegal activity directed at anyone, including people running for elected office, is unacceptable. I endorse and echo the comments they made in their very powerful and moving speeches.

In relation to the technicality of these amendments, what they are asking for is in the Bill already but in different places. This clause is about protecting content of "democratic importance" and concerns stopping

online social media firms deleting content through over-zealous takedown. What the hon. Members are talking about is different. They are talking about abuse and illegal activities, such as rape threats, that people get on social media, particularly female MPs, as they both pointed out. I can point to two other places in the Bill where what they are asking for is delivered.

First, there are the duties around illegal content that we debated this morning. If there is content online that is illegal—some of the stuff that the shadow Minister referred to earlier sounds as if it would meet that threshold—then in the Bill there is a duty on social media firms to remove that content and to proactively prevent it if it is on the priority list. The route to prosecution will exist in future, as it does now, and the user-verification measures, if a user is verified, make it more likely for the police to identify the person responsible. In the context of identifying people carrying out abuse, I know the Home Office is looking at the Investigatory Powers Act 2016 as a separate piece of work that speaks to that issue.

So illegal content is dealt with in the illegal content provisions in the Bill, but later we will come to clause 150, which updates the Malicious Communications Act 1988 and creates a new harmful communications offence. Some of the communications that have been described may not count as a criminal offence under other parts of criminal law, but if they meet the test of harmful communication in clause 150, they will be criminalised and will therefore have to be taken down, and prosecution will be possible. In meeting the very reasonable requests that the hon. Members for Batley and Spen and for Aberdeen North have made, I would point to those two parts of the Bill.

Kirsty Blackman: But clause 150(5) says that if a message

"is, or is intended to be, a contribution to a matter of public interest",

people are allowed to send it, which basically gives everybody a get-out clause in relation to anything to do with elections.

Chris Philp: No, it does not.

Kirsty Blackman: I know we are not discussing that part of the Bill, and if the Minister wants to come back to this when we get to clause 150, I have no problem with that.

Chris Philp: I will answer the point now, as it has been raised. Clause 150 categorically does not give a get-out-of-jail-free card or provide an automatic excuse. Clearly, there is no way that abusing a candidate for elected office with rape threats and so on could possibly be considered a matter of public interest. In fact, even if the abuse somehow could be considered as possibly contributing to public debate, clause 150(5) says explicitly in line 32 on page 127:

"but that does not determine the point".

Even where there is some potentially tenuous argument about a contribution to a matter of public interest, which most definitely would not be the case for the rape threats that have been described, that is not determinative. It is a balancing exercise that gets performed, and I hope that puts the hon. Lady's mind at rest.

Kim Leadbeater: The Minister makes a really valid point and is right about the impact on the individual. The point I am trying to make with the amendments is that this is about the impact on the democratic process, which is why I think it fits in with clause 15. It is not about how individuals feel; it is about the impact that that has on behaviours, and about putting the emphasis and onus on platforms to decide what is of democratic importance. In the evidence we had two weeks ago, the witnesses certainly did not feel comfortable with putting the onus on platforms. If we were to have a code of practice, we would at least give them something to work with on the issue of what is of democratic importance. It is about the impact on democracy, not just the harm to the individual involved.

Chris Philp: Clearly, if a communication is sufficiently offensive that it meets the criminal threshold, it is covered, and that would obviously harm the democratic process as well. If a communication was sufficiently offensive that it breached the harmful communication offence in clause 150, it would also, by definition, harm the democratic process, so communications that are damaging to democracy would axiomatically be caught by one thing or the other. I find it difficult to imagine a communication that might be considered damaging to democracy but that would not meet one of those two criteria, so that it was not illegal and would not meet the definition of a harmful communication.

My main point is that the existing provisions in the Bill address the kinds of behaviours that were described in those two speeches—the illegal content provisions, and the new harmful communication offence in clause 150. On that basis, I hope the hon. Member for Batley and Spen will withdraw the amendment, safe in the knowledge that the Bill addresses the issue that she rightly and reasonably raises.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 13]

AYES

Blackman, Kirsty	Keeley, Barbara
Carden, Dan	Leadbeater, Kim
Davies-Jones, Alex	Mishra, Navendu

NOES

Ansell, Caroline	Miller, rh Dame Maria
Bailey, Shaun	Moore, Damien
Double, Steve	Philp, Chris
Fletcher, Nick	Stevenson, Jane
Holden, Mr Richard	

Question accordingly negatived.

Question proposed, That the clause stand part of the Bill.

The Chair: With this it will be convenient to discuss the following:

Clause 16 stand part.

New clause 7—*Report on duties to protect content of democratic importance and journalistic content—*

"(1) The Secretary of State must publish a report which—

(a) reviews the extent to which Category 1 services have fulfilled their duties under—

(i) Clause 15; and

(ii) Clause 16;

(b) analyses the effectiveness of Clauses 15 and 16 in protecting against—

(i) foreign state actors;

(ii) extremist groups and individuals; and

(iii) sources of misinformation and disinformation.

(2) The report must be laid before Parliament within one year of this Act being passed."

This new clause would require the Secretary of State to publish a report reviewing the effectiveness of Clauses 15 and 16.

4.45 pm

Alex Davies-Jones: I will speak to clauses 15 and 16 and to new clause 7. The duties outlined in the clause, alongside clause 16, require platforms to have special terms and processes for handling journalistic and democratically important content. In respect of journalistic content, platforms are also required to provide an expedited appeals process for removed posts, and terms specifying how they will define journalistic content. There are, however, widespread concerns about both those duties.

As the Bill stands, we feel that there is too much discretion for platforms. They are required to define "journalistic" content, a role that they are completely unsuited to and, from what I can gather, do not want. In addition, the current drafting leaves the online space open to abuse. Individuals intent on causing harm are likely to apply to take advantage of either of those duties; masquerading as journalists or claiming democratic importance in whatever harm they are causing, and that could apply to almost anything. In the evidence sessions, we also heard about the concerns expressed brilliantly by Kyle Taylor from Fair Vote and Ellen Judson from Demos, that the definitions as they stand in the Bill thus far are broad and vague. However, we will come on to those matters later.

Ultimately, treating "journalistic" and "democratically important" content differently is unworkable, leaving platforms to make impossible judgments over, for example, when and for how long an issue becomes a matter of reasonable public debate, or in what settings a person is acting as a journalist. As the Minister knows, the duties outlined in the clause could enable a far-right activist who was standing in an election, or potentially even just supporting candidates in elections, to use all social media platforms. That might allow far-right figures to be re-platformed on to social media sites where they would be free to continue spreading hate.

The Bill indicates that content will be protected if created by a political party ahead of a vote in Parliament, an election or a referendum, or when campaigning on a live political issue—basically, anything. Can the Minister confirm whether the clause means that far-right figures who have been de-platformed for hate speech already must be reinstated if they stand in an election? Does that include far-right or even neo-Nazi political parties? Content and accounts that have been de-platformed from mainstream platforms for breaking terms of service should not be allowed to return to those platforms via this potential—dangerous—loophole.

As I have said, however, I know that these matters are complex and, quite rightly, exemptions must be in place to allow for free discussion around matters of the day. What cannot be allowed to perpetuate is hate sparked by bad actors using simple loopholes to avoid any consequences.

On clause 16, the Minister knows about the important work that Hope not Hate is doing in monitoring key far-right figures. I pay tribute to it for its excellent work. Many of them self-define as journalists and could seek to exploit this loophole in the Bill and propagate hate online. Some of the most high-profile and dangerous far-right figures in the UK, including Stephen Yaxley-Lennon, also known as Tommy Robinson, now class themselves as journalists. There are also far-right and conspiracy-theory so-called "news companies" such as Rebel Media and Urban Scoop. Both those replicate mainstream news publishers, but are used to spread misinformation and discriminatory content. Many of those individuals and organisations have been de-platformed already for consistently breaking the terms of service of major social media platforms, and the exemption could see them demand their return and have their return allowed.

New clause 7 would require the Secretary of State to publish a report reviewing the effectiveness of clauses 15 and 16. It is a simple new clause to require parliamentary scrutiny of how the Government's chosen means of protecting content of democratic importance and content of journalistic content are working.

Hacked Off provided me with a list of people it found who have claimed to be journalists and who would seek to exploit the journalistic content duty, despite being banned from social media because they are racists or bad actors. First is Charles C. Johnson, a far-right activist who describes himself as an "investigative journalist". Already banned from Twitter for saying he would "take out" a civil rights activist, he is also alleged to be a holocaust denier.

Secondly, we have Robert Stacy McCain. Robert has been banned from Twitter for participating in targeted abuse. He was a journalist for *The Washington Post*, but is alleged to have also been a member of the League of the South, a far-right group known to include racists. Then, there is Richard B. Spencer, a far-right journalist and former editor, only temporary banned for using overlapping accounts. He was pictured making the Nazi salute and has repeated Nazi propaganda. When Trump became President, he encouraged people to "party like it's 1933". Sadly, the list goes on and on.

Transparency is at the very heart of the Bill. The Minister knows we have concerns about clauses 15 and 16, as do many of his own Back Benchers. We have heard from my hon. Friend the Member for Batley and Spen how extremist groups and individuals and foreign state actors are having a very real impact on the online space. If the Minister is unwilling to move on tightening up those concepts, the very least he could commit to is a review that Parliament will be able to formally consider.

Chris Philp: I thank the shadow Minister for her comments and questions. I would like to pick up on a few points on the clauses. First, there was a question about what content of democratic importance and content of journalistic importance mean in practice. As with many concepts in the Bill, we will look to Ofcom to issue codes of practice specifying precisely how we might expect platforms to implement the various provisions in the Bill. That is set out in clause 37(10)(e) and (f), which appear at the top of page 37, for ease. Clauses 15

and 16 on content of democratic and journalistic importance are expressly referenced as areas where codes of practice will have to be published by Ofcom, which will do further work on and consult on that. It will not just publish it, but will go through a proper process.

The shadow Minister expressed some understandable concerns a moment ago about various extremely unpleasant people, such as members of the far right who might somehow seek to use the provisions in clauses 15 and 16 as a shield behind which to hide, to enable them to continue propagating hateful, vile content. I want to make it clear that the protections in the Bill are not absolute—it is not that if someone can demonstrate that what they are saying is of democratic importance, they can say whatever they like. That is not how the clauses are drafted.

I draw attention to subsection (2) of both clauses 15 and 16. At the end of the first block of text, just above paragraph (a), it says "taken into account": the duty is to ensure that matters concerning the importance of freedom of expression relating to content of democratic importance are taken into account when making decisions. It is not an absolute prohibition on takedown or an absolute protection, but simply something that has to be taken into account.

If someone from the far right, as the shadow Minister described, was spewing out vile hatred, racism or antisemitism, and tried to use those clauses, the fact that they might be standing in an election might well be taken into account. However, in performing that balancing exercise, the social media platforms and Ofcom acting as enforcers—and the court if it ever got judicially reviewed—would weigh those things up and find that taking into account content of democratic importance would not be sufficient to outweigh considerations around vile racism, antisemitism or misogyny.

Alex Davies-Jones: The Minister mentions that it would be taken into account. How long does he anticipate it would be taken into account for, especially given the nature of an election? A short campaign could be a number of weeks, or something could be posted a day before an election, be deemed democratically important and have very serious and dangerous ramifications.

Chris Philp: As I say, if content was racist, antisemitic or flagrantly misogynistic, the balancing exercise is performed and the democratic context may be taken into account. I do not think the scales would tip in favour of leaving the content up. Even during an election period, I think common sense dictates that.

To be clear on the timing point that the hon. Lady asked about, the definition of democratic importance is not set out in hard-edged terms. It does not say, "Well, if you are in a short election period, any candidate's content counts as of democratic importance." It is not set out in a manner that is as black and white as that. If, for example, somebody was a candidate but it was just racist abuse, I am not sure how even that would count as democratic importance, even during an election period, because it would just be abuse; it would not be contributing to any democratic debate. Equally, somebody might not be a candidate, or might have been a candidate historically, but might be contributing to a legitimate debate after an election. That might be seen as being of democratic importance, even though they were not actually a candidate. As I said, the concept is not quite as black and white as that. The main point is that it is only to be taken into account; it is not determinative.

Alex Davies-Jones: I appreciate the Minister's allowing me to come back on this. During the Committee's evidence sessions, we heard of examples where bad-faith state actors were interfering in the Scottish referendum, hosting Facebook groups and perpetuating disinformation around the royal family to persuade voters to vote "Yes" to leave the United Kingdom. That disinformation by illegal bad-faith actors could currently come under both the democratic importance and journalistic exemptions, so would be allowed to remain for the duration of that campaign. Given the exemptions in the Bill, it could not be taken down but could have huge, serious ramifications for democracy and the security of the United Kingdom.

Chris Philp: I understand the points that the hon. Lady is raising. However, I do not think that it would happen in that way.

Alex Davies-Jones: You don't think?

Chris Philp: No, I don't. First of all, as I say, it is taken into account; it is not determinative. Secondly, on the point about state-sponsored disinformation, as I think I mentioned yesterday in response to the hon. Member for Liverpool, Walton, there is, as we speak, a new criminal offence of foreign interference being created in the National Security Bill. That will criminalise the kind of foreign interference in elections that she referred to. Because that would then create a new category of illegal content, that would flow through into this Bill. That would not be overridden by the duty to protect content of democratic importance set out here. I think that the combination of the fact that this is a balancing exercise, and not determinative, and the new foreign interference offence being created in the National Security Bill, will address the issue that the hon. Lady is raising—reasonably, because it has happened in this country, as she has said.

I will briefly turn to new clause 7, which calls for a review. I understand why the shadow Minister is proposing a review, but there is already a review mechanism in the Bill; it is to be found in clause 149, and will, of course, include a review of the way that clauses 15 and 16 operate. They are important clauses; we all accept that journalistic content and content of democratic importance is critical to the functioning of our society. Case law relating to article 10 of the European convention on human rights, for example, recognises content of journalistic importance as being especially critical. These two clauses seek to ensure that social media firms, in making their decisions, and Ofcom, in enforcing the firms, take account of that. However, it is no more than that: it is "take account", it is not determinative.

Question put and agreed to.

Clause 15 accordingly ordered to stand part of the Bill.

Clause 16 ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned. *—(Steve Double.)*

4.59 pm

Adjourned till Thursday 9 June at half-past Eleven o'clock.

Written evidence to be reported to the House

OSB39 LV=General Insurance

OSB40 Epilepsy Society

OSB41 Free Speech Union

OSB42 Graham Smith

OSB43 Center for Data Innovation

OSB44 Samaritans

OSB45 End Violence Against Women coalition, Glitch, Refuge, Carnegie UK, 5Rights, NSPCC and Professors Lorna Woods and Clare McGlynn (joint submission)

OSB46 Sky

OSB47 Peter Wright, Editor Emeritus, DMG Media

OSB48 Graham Smith (further submission)

OSB49 CARE (Christian Action Research and Education)

OSB50 Age Verification Providers Association (supplementary submission)

OSB51 Legal Advice Centre at Queen Mary, University of London and Mishcon de Reya LLP (joint submission)

OSB52 Google UK (supplementary submission)

OSB53 Refuge (supplementary submission)

OSB54 Reset (supplementary submission)

OSB55 Public Service Broadcasters (BBC, Channel 4, and Channel 5)

OSB56 Which?

OSB57 Professor Corinne Fowler, School of Museum Studies, University of Leicester

OSB58 Independent Media Association

OSB59 Hacked Off Campaign

OSB60 Center for Countering Digital Hate