PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

ONLINE SAFETY BILL

Twelfth Sitting

Thursday 16 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

Monday 20 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

Thursday 16 June 2022

(Afternoon)

[Sir Roger Gale *in the Chair*]

Online Safety Bill

Clause 103

Notices to deal with terrorism content or CSEA content (or both)

2 pm

The Chair: There are amendments to clause 103 that are not owned by any member of the Committee. Nobody has indicated that they wish to take them up, and therefore they fall.

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

The Chair: With this it will be convenient to consider clauses 105 and 106 stand part.

Alex Davies-Jones (Pontypridd) (Lab): Under this chapter, Ofcom will have the power to direct companies to use accredited technology to identify child sexual exploitation and abuse content, whether communicated publicly or privately by means of a service, and to remove that content quickly. Colleagues will be aware that the Internet Watch Foundation is one group that assists companies in doing that by providing them with "hashes" of previously identified child sexual abuse material in order to prevent the upload of such material to their platforms. That helps stop the images of victims being recirculated again and again. Tech companies can then notify law enforcement of the details of who has uploaded the content, and an investigation can be conducted and offenders sharing the content held to account.

Those technologies are extremely accurate and, thanks to the quality of our datasets, ensure that companies are detecting only imagery that is illegal. There are a number of types of technology that Ofcom could consider accrediting, including image hashing. A hash is a unique string of letters and numbers that can be applied to an image and matched every time a user attempts to upload a known illegal image to a platform.

PhotoDNA is another type, created in 2009 in a collaboration between Microsoft and Professor Hany Farid at the University of Berkeley. PhotoDNA is a vital tool in the detection of CSEA online. It enables law enforcement, charities, non-governmental organisations and the internet industry to find copies of an image even when it has been digitally altered. It is one of the most important technical developments in online child protection. It is extremely accurate, with a failure rate of one in 50 billion to 100 billion. That gives companies a high degree of certainty that what they are removing is illegal, and a firm basis for law enforcement to pursue offenders.

Lastly, there is webpage blocking. Most of the imagery that the Internet Watch Foundation removes from the internet is hosted outside the UK. While it is waiting for removal, it can disable public access to an image or webpage by adding it to our webpage blocking list. That can be utilised by search providers to de-index known webpages containing CSAM. I therefore ask the Minister, as we continue to explore this chapter, to confirm exactly how such technologies can be utilised once the Bill receives Royal Assent.

Labour welcomes clause 105, which confirms, in subsection (2), that where a service provider is already using technology on a voluntary basis but it is ineffective, Ofcom can still intervene and require a service provider to use a more effective technology, or the same technology in a more effective way. It is vital that Ofcom is given the power and opportunity to intervene in the strongest possible sense to ensure that safety online is kept at the forefront.

However, we do require some clarification, particularly on subsections (9) and (10), which explain that Ofcom will only be able to require the use of tools that meet the minimum standards for accuracy for detecting terrorism and/or CSEA content, as set out by the Secretary of State. Although minimum standards are of course a good thing, can the Minister clarify the exact role that the Secretary of State will have in imposing these minimum standards? How will this work in practice?

Once again, Labour does not oppose clause 106 and we have not sought to amend it at this stage. It is vital that Ofcom has the power to revoke a notice under clause 103(1) if there are reasonable grounds to believe that the provider is not complying with it. Only with these powers can we be assured that service providers will be implored to take their responsibilities and statutory duties, as outlined in the Bill, seriously.

Kirsty Blackman (Aberdeen North) (SNP): I have a few questions, concerns and suggestions relating to these clauses. I think it was the hon. Member for Don Valley who asked me last week about the reports to the National Crime Agency and how that would work—about how, if a human was not checking those things, there would be an assurance that proper reports were being made, and that scanning was not happening and reports were not being made when images were totally legal and there was no problem with them. *[Interruption.]* I thought it was the hon. Member for Don Valley, although it may not have been. Apologies—it was a Conservative Member. I am sorry for misnaming the hon. Member.

The hon. Member for Pontypridd made a point about the high level of accuracy of the technologies. That should give everybody a level of reassurance that the reports that are and should be made to the National Crime Agency on child sexual abuse images will be made on a highly accurate basis, rather than a potentially inaccurate one. Actually, some computer technology—particularly for scanning for images, rather than text—is more accurate than human beings. I am pleased to hear those particular statistics.

Queries have been raised on this matter by external organisations—I am particularly thinking about the NSPCC, which we spoke about earlier. The Minister has thankfully given a number of significant reassurances about the ability to proactively scan. External organisations

such as the NSPCC are still concerned that there is not enough on the face of the Bill about proactive scanning and ensuring that the current level of proactive scanning is able—or required—to be replicated when the Bill comes into action.

During an exchange in an earlier Committee sitting, the Minister gave a commitment—I am afraid I do not have the quote—to being open to looking at amending clause 103. I am slightly disappointed that there are no Government amendments, but I understand that there has been only a fairly short period; I am far less disappointed than I was previously, when the Minister had much more time to consider the actions he might have been willing to take.

The suggestion I received from the NSPCC is about the gap in the Bill regarding the ability of Ofcom to take action. These clauses allow Ofcom to take action against individual providers about which it has concerns; those providers will have to undertake duties set out by Ofcom. The NSPCC suggests that there could be a risk register, or that a notice could be served on a number of companies at one time, rather than Ofcom simply having to pick one company, or to repeatedly pick single companies and serve notices on them. Clause 83 outlines a register of risk profiles that must be created by Ofcom. It could therefore serve notice on all the companies that fall within a certain risk profile or all the providers that have common functionalities.

If there were a new, emerging concern, that would make sense. Rather than Ofcom having to go through the individual process with all the individual providers when it knows that there is common functionality—because of the risk assessments that have been done and Ofcom's oversight of the different providers—it could serve notice on all of them in one go. It could not then accidentally miss one out and allow people to move to a different platform that had not been mentioned. I appreciate the conversation we had around this issue earlier, and the opportunity to provide context in relation to the NSPCC's suggestions, but it would be great if the Minister would be willing to consider them.

I have another question, to which I think the Minister will be able to reply in the affirmative, which is on the uses of the technology as it evolves. We spoke about that in an earlier meeting. The technology that we have may not be what we use in the future to scan for terrorist-related activity or child sexual abuse material. It is important that the Bill adequately covers future conditions. I think that it does, but will the Minister confirm that, as technology advances and changes, these clauses will adequately capture the scanning technologies that are required, and any updates in the way in which platforms work and we interact with each other on the internet?

I have fewer concerns about future-proofing with regard to these provisions, because I genuinely think they cover future conditions, but it would be incredibly helpful and provide me with a bit of reassurance if the Minister could confirm that. I very much look forward to hearing his comments on clause 103.

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Chris Philp): Let me start by addressing some questions raised by hon. Members, beginning with the last point made by the hon. Member for Aberdeen North. She sought reconfirmation that the Bill will keep up with future developments in accredited technology that are not currently contemplated. The answer to her question can be found in clause 105(9), in which the definition of accredited technology is clearly set out, as technology that is

"accredited (by OFCOM or another person appointed by OFCOM) as meeting minimum standards of accuracy".

That is not a one-off determination; it is a determination, or an accreditation, that can happen from time to time, periodically or at any point in the future. As and when new technologies emerge that meet the minimum standards of accuracy, they can be accredited, and the power in clause 103 can be used to compel platforms to use those technologies. I hope that provides the reassurance that the hon. Member was quite rightly asking for.

The shadow Minister, the hon. Member for Pontypridd, asked a related question about the process for publishing those minimum standards. The process is set out in clause 105(10), which says that Ofcom will give advice to the Secretary of State on the appropriate minimum standards, and the minimum standards will then be

"approved…by the Secretary of State, following advice from OFCOM."

We are currently working with Ofcom to finalise the process for setting those standards, which of course will need to take a wide range of factors into account.

Let me turn to the substantive clauses. Clause 103 is extremely important, because as we heard in the evidence sessions and as Members of the Committee have said, scanning messages using technology such as hash matching, to which the shadow Minister referred, is an extremely powerful way of detecting CSEA content and providing information for law enforcement agencies to arrest suspected paedophiles. I think it was in the European Union that Meta—particularly Facebook and Facebook Messenger—stopped using this scanner for a short period time due to misplaced concerns about privacy laws, and the number of referrals of CSEA images and the number of potential paedophiles who were referred to law enforcement dropped dramatically.

A point that the hon. Member for Aberdeen North and I have discussed previously is that it would be completely unacceptable if a situation arose whereby these messages—I am thinking particularly about Facebook Messenger—did not get scanned for CSEA content in a way that they do get scanned today. When it comes to preventing child sexual exploitation and abuse, in my view there is no scope for compromise or ambiguity. That scanning is happening at the moment; it is protecting children on a very large scale and detecting paedophiles on quite a large scale. In my view, under no circumstances should that scanning be allowed to stop. That is the motivation behind clause 103, which provides Ofcom with the power to make directions to require the use of accredited technology.

As the hon. Member for Aberdeen North signalled in her remarks, given the importance of this issue the Government are of course open to thinking about ways in which the Bill can be strengthened if necessary, because we do not want to leave any loopholes. I urge any social media firms watching our proceedings never to take any steps that degrade or reduce the ability to scan for CSEA content. I thank the hon. Member for sending through the note from the NSPCC, which I have received and will look at internally.

2.15 pm

The proactive scanning that we have talked about is critical. To give one or two examples, this is not just about CSEA, but terrorism as well. Every terrorist attack in 2017 had an online element, and many counter-terrorism prosecutions have involved online activity, because terrorists and their supporters continue to use a wide range of online platforms to further their aims. Similarly, in the context of child sexual abuse material, the Internet Watch Foundation confirmed in 2020 that 153,383 reports of webpages containing CSEA, abuse imagery or UK-hosted, non-photographic child sexual abuse imagery were detected. The importance of the scanning technology is clear, as is the importance of ensuring the clause is as strong as possible.

As the shadow Minister has said, clause 105 provides supporting provisions for clause 103, setting out—for example—the particulars of what must appear in the notice, and clause 106 sets out the process for reviewing a notice to deal with terrorism or CSEA content. I hope I have addressed hon. Members' questions, and I commend this important clause to the Committee.

Question put and agreed to.

Clause 103 accordingly ordered to stand part of the Bill.

Clause 104

MATTERS RELEVANT TO A DECISION TO GIVE A NOTICE UNDER SECTION 103(1)

Alex Davies-Jones: I beg to move amendment 35, in clause 104, page 88, line 39, leave out "prevalence" and insert "presence".

This amendment requires that Ofcom considers the presence of relevant content, rather than its prevalence.

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

Amendment 36, in clause 104, page 88, line 43, leave out "prevalence" and insert "presence".

This amendment requires that Ofcom considers the presence of relevant content, rather than its prevalence.

Amendment 37, in clause 104, page 89, line 13, at end insert—

"(k) risk of harm posed by individuals in the United Kingdom in relation to adults and children in the UK or elsewhere through the production, publication and dissemination of illegal content."

This amendment requires the Ofcom's risk assessment to consider risks to adults and children through the production, publication and dissemination of illegal content.

Amendment 39, in clause 116, page 98, line 37, leave out "prevalence" and insert "presence".

This amendment requires that Ofcom considers the presence of relevant content, rather than its prevalence.

Amendment 40, in clause 116, page 98, line 39, leave out "prevalence" and insert "presence".

This amendment requires that Ofcom considers the presence of relevant content, rather than its prevalence.

Amendment 38, in clause 116, page 99, line 12, at end insert—

"(j) the risk of harm posed by individuals in the United Kingdom in relation to adults and children in the UK or elsewhere through the production, publication and dissemination of illegal content."

This amendment requires Ofcom to consider risks to adults and children through the production, publication and dissemination of illegal content before imposing a proactive technology requirement.

Government amendment 6.

Clause stand part.

Alex Davies-Jones: We welcome clause 104, but have tabled some important amendments that the Minister should closely consider. More broadly, the move away from requiring child sexual exploitation and abuse content to be prevalent and persistent before enforcement action can be taken is a positive one. It is welcome that Ofcom will have the opportunity to consider a range of factors.

Despite this, Labour—alongside the International Justice Mission—is still concerned about the inclusion of prevalence as a factor, owing to the difficulty in detecting newly produced CSEA content, especially livestreamed abuse. Amendments 35, 36, 39 and 40 seek to address that gap. Broadly, the amendments aim to capture the concern about the Bill's current approach, which we feel limits its focus to the risk of harm faced by individuals in the UK. Rather, as we have discussed previously, the Bill should recognise the harm that UK nationals cause to people around the world, including children in the Philippines. The amendments specifically require Ofcom to consider the presence of relevant content, rather than its prevalence.

Amendment 37 would require Ofcom's risk assessments to consider risks to adults and children through the production, publication and dissemination of illegal content—an issue that Labour has repeatedly raised. I believe we last mentioned it when we spoke to amendments to clause 8, so I will do my best to not repeat myself. That being said, we firmly believe it is important that video content, including livestreaming, is captured by the Bill. I remain unconvinced that the Bill as it stands goes far enough, so I urge the Minister to closely consider and support these amendments. The arguments that we and so many stakeholders have already made still stand.

Kirsty Blackman: I echo the sentiments that have been expressed by the shadow Minister, and thank her and her colleagues for tabling this amendment and giving voice to the numerous organisations that have been in touch with us about this matter. The Scottish National party is more than happy to support the amendment, which would make the Bill stronger and better, and would better enable Ofcom to take action when necessary.

Chris Philp: I understand the spirit behind these amendments, focusing on the word "presence" rather than "prevalence" in various places. It is worth keeping in mind that throughout the Bill we are requiring companies to implement proportionate systems and processes to protect their users from harm. Even in the case of the most harmful illegal content, we are not placing the duty on companies to remove every single piece of illegal content that has ever appeared online, because that is requesting the impossible. We are asking them to take reasonable and proportionate steps to create systems and processes to do so. It is important to frame the legally binding duties in that way that makes them realistically achievable.

As the shadow Minister said, amendments 35, 36, 39 and 40 would replace the word "prevalence" with "presence". That would change Ofcom's duty to enforce

not just against content that was present in significant numbers—prevalent—but against a single instance, which would be enough to engage the clause.

We mutually understand the intention behind these amendments, but we think the significant powers to compel companies to adopt certain technology contained in section 103 should be engaged only where there is a reasonable level of risk. For example, if a single piece of content was present on a platform, if may not be reasonable or proportionate to force the company to adopt certain new technologies, where indeed they do not do so at the moment. The use of "prevalence" ensures that the powers are used where necessary.

It is clear—there is no debate—that in the circumstances where scanning technology is currently used, which includes on Facebook Messenger, there is enormous prevalence of material. To elaborate on a point I made in a previous discussion, anything that stops that detection happening would be unacceptable and, in the Government's view, it would not be reasonable to lose the ability to detect huge numbers of images in the service of implementing encryption, because there is nothing more important than scanning against child sexual exploitation images.

However, we think adopting the amendment and replacing the word "prevalence" with "presence" would create an extremely sensitive trigger that would be engaged on almost every site, even tiny ones or where there was no significant risk, because a single example would be enough to trigger the amendment, as drafted. Although I understand the spirit of the amendment, it moves away from the concepts of proportionality and reasonableness in the systems and processes that the Bill seeks to deliver.

Amendment 37 seeks to widen the criteria that Ofcom must consider when deciding to use section 103 powers. It is important to ensure that Ofcom considers a wide range of factors, taking into account the harm occurring, but clause 104(2)(f) already requires Ofcom to consider "the level of risk of harm to individuals in the United Kingdom presented by relevant content, and the severity of that harm". Therefore, the Bill already contains provision requiring Ofcom to take those matters into account, as it should, but the shadow Minister is right to draw attention to the issue.

Finally, amendment 38 seeks to amend clause 116 to require Ofcom to consider the risk of harm posed by individuals in the United Kingdom, in relation to adults and children in the UK or elsewhere, through the production, publication and dissemination of illegal content. In deciding whether to make a confirmation decision requiring the use of technology, it is important that Ofcom considers a wide range of factors. However, clause 116(6)(e) already proposes to require Ofcom to consider, in particular, the risk and severity of harm to individuals in the UK. That is clearly already in the Bill.

I hope that this analysis provides a basis for the shadow Minister to accept that the Bill, in this area, functions as required. I gently request that she withdraw her amendment.

Alex Davies-Jones: I welcome the Minister's comments, but if we truly want the Bill to be world-leading, as the Government and the Minister insist it will be, and if it is truly to keep children safe, surely one image of child sexual exploitation and abuse on a platform is one too many. We do not need to consider prevalence over presence. I do not buy that argument. I believe we need to do all we can to make this Bill as strong as possible. I believe the amendments would do that.

Question put, That the amendment be made.

The Committee divided: Ayes 3, Noes 5.

Division No. 33]

AYES

Blackman, Kirsty	Keeley, Barbara
Davies-Jones, Alex	

NOES

Bailey, Shaun	Philp, Chris
Fletcher, Nick	
Miller, rh Dame Maria	Russell, Dean

Question accordingly negatived.

Amendment proposed: 37, in clause 104, page 89, line 13, at end insert—

"(k) risk of harm posed by individuals in the United Kingdom in relation to adults and children in the UK or elsewhere through the production, publication and dissemination of illegal content."—*(Alex Davies-Jones.)*

This amendment requires the Ofcom's risk assessment to consider risks to adults and children through the production, publication and dissemination of illegal content.

Question put, That the amendment be made.

The Committee divided: Ayes 3, Noes 5.

Division No. 34]

AYES

Blackman, Kirsty	Keeley, Barbara
Davies-Jones, Alex	

NOES

Bailey, Shaun	Philp, Chris
Fletcher, Nick	
Miller, rh Dame Maria	Russell, Dean

Question accordingly negatived.

Chris Philp: I beg to move amendment 6, in clause 104, page 89, line 14, after "(2)(f)" insert ", (g)"

This amendment ensures that subsection (3) of this clause (which clarifies what "relevant content" in particular paragraphs of subsection (2) refers to in relation to different kinds of services) applies to the reference to "relevant content" in subsection (2)(g) of this clause.

This technical amendment will ensure that the same definition of "relevant content" used in subsection (2) is used in subsection (3).

Amendment 6 agreed to.

Clause 104, as amended, ordered to stand part of the Bill.

Clauses 105 and 106 ordered to stand part of the Bill.

Clause 107

OFCOM'S GUIDANCE ABOUT FUNCTIONS UNDER THIS CHAPTER

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

The Chair: With this it will be convenient to discuss clauses 108 and 109 stand part.

Alex Davies-Jones: Labour welcomes clause 107, which requires Ofcom to issue guidance setting out the circumstances in which it could require a service provider in scope of the power to use technology to identify CSEA and/or terrorism content. It is undeniably important that Ofcom will have the discretion to decide on the exact content of the guidance, which it must keep under review and publish.

We also welcome the fact that Ofcom must have regard to its guidance when exercising these powers. Of course, it is also important that the Information Commissioner is included and consulted in the process. Ofcom has a duty to continually review its guidance, which is fundamental to the Bill's success.

We also welcome clause 108. Indeed, the reporting of Ofcom is an area that my hon. Friend the Member for Batley and Spen will touch on when we come to new clause 25. It is right that Ofcom will have a statutory duty to lay an annual report in this place, but we feel it should ultimately go further. That is a conversation for another day, however, so we broadly welcome clause 108 and have not sought to amend it directly at this stage.

Clause 109 ensures that the definitions of "terrorism content" and "child sexual exploitation and abuse content" used in chapter 5 are the same as those used in part 3. Labour supports the clause and we have not sought to amend it.

2.30 pm

The Chair: The Question is—

Kirsty Blackman *rose—*

The Chair: I beg your pardon; I am trying to do too many things at once. I call Kirsty Blackman.

Kirsty Blackman: Thank you very much, Sir Roger. I do not envy you in this role, which cannot be easy, particularly with a Bill that is 190-odd clauses long.

The Chair: It goes with the job.

Kirsty Blackman: I have a quick question for the Minister about the timelines in relation to the guidance and the commitment that Ofcom gave to producing a road map before this coming summer. When is that guidance likely to be produced? Does that road map relate to the guidance in this clause, as well as the guidance in other clauses? If the Minister does not know the answer, I have no problem with receiving an answer at a later time. Does the road map include this guidance as well as other guidance that Ofcom may or may not be publishing at some point in the future?

Chris Philp: I welcome the cross-party support for the provisions set out in these important clauses. Clause 107 points out the requirement for Ofcom to publish guidance, which is extremely important. Clause 108 makes sure that it publishes an annual report. Clause 109 covers the interpretations.

The hon. Member for Aberdeen North asked the only question, about the contents of the Ofcom road map, which in evidence it committed to publishing before the summer. I cannot entirely speak for Ofcom, which is of course an independent body. In order to avoid me giving the Committee misleading information, the best thing is for officials at the Department for Digital, Culture, Media and Sport to liaise with Ofcom and ascertain what the exact contents of the road map will be, and we can report that back to the Committee by letter.

It will be fair to say that the Committee's feeling—I invite hon. Members to intervene if I have got this wrong—is that the road map should be as comprehensive as possible. Ideally, it would lay out the intended plan to cover all the activities that Ofcom would have to undertake in order to make the Bill operational, and the more detail there is, and the more comprehensive the road map can be, the happier the Committee will be.

Officials will take that away, discuss it with Ofcom and we can revert with fuller information. Given that the timetable was to publish the road map prior to the summer, I hope that we are not going to have to wait very long before we see it. If Ofcom is not preparing it now, it will hopefully hear this discussion and, if necessary, expand the scope of the road map a little bit accordingly.

Question put and agreed to.

Clause 107 accordingly ordered to stand part of the Bill

Clauses 108 and 109 ordered to stand part of the Bill.

Clause 110

PROVISIONAL NOTICE OF CONTRAVENTION

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

Alex Davies-Jones: I will be brief. Labour welcomes clause 110, which addresses the process of starting enforcement. We support the process, particularly the point that ensures that Ofcom must first issue a "provisional notice of contravention" to an entity before it reaches its final decision.

The clause ultimately ensures that the process for Ofcom issuing a provisional notice of contravention can take place only after a full explanation and deadline has been provided for those involved. Thankfully, this process means that Ofcom can reach a decision only after allowing the recipient a fair opportunity to make relevant representations too. The process must be fair for all involved and that is why we welcome the provisions outlined in the clause.

Dame Maria Miller (Basingstoke) (Con): I hope that I am speaking at the right stage of the Bill, and I promise not to intervene at any further stages where this argument could be put forward.

Much of the meat of the Bill is within chapter 6. It establishes what many have called the "polluter pays" principle, where an organisation that contravenes can then be fined—a very important part of the Bill. We are talking about how Ofcom is going to be able to make the provisions that we have set out work in practice. A regulated organisation that fails to stop harm contravenes and will be fined, and fined heavily.

I speak at this point in the debate with slight trepidation, because these issues are also covered in clause 117 and schedule 12, but it is just as relevant to debate the point at this stage. It is difficult to understand where in the Bill the Government set out how the penalties that they can levy as a result of the powers under this clause will be used. Yes, they will be a huge deterrent, and that is good in its own right and important, but surely the real opportunity is to make the person who does the harm pay for righting the wrong that they have created.

That is not a new concept. Indeed, it is one of the objectives that the Government set out in the intentions behind their approach to the draft victims Bill. It is a concept used in the Investigatory Powers Act 2016. It is the concept behind the victims surcharge. So how does this Bill make those who cause harm take greater responsibility for the cost of supporting victims to recover from what they have suffered? That is exactly what the Justice Ministers set out as being so important in their approach to victims. In the Bill, that is not clear to me.

At clause 70, the Minister helpfully set out that there was absolutely no intention for Ofcom to have a role in supporting victims individually. In reply to the point that I made at that stage, he said that the victims Bill would address some of the issues—I am sure that he did not say all the issues, but some of them at least. I do not believe that it will. The victims Bill establishes a code and a duty to provide victim support, but it makes absolutely no reference to how financial penalties on those who cause harm—as set out so clearly in this Bill—will be used to support victims. How will they support victims' organisations, which do so much to help in particular those who do not end up in court, before a judge, because what they have suffered does not warrant that sort of intervention?

I believe that there is a gap. We heard that in our evidence session, including from Ofcom itself, which identified the need for law enforcement, victim-support organisations and platforms themselves to find what the witnesses described as an effective way for the new "ecosystem" to work. Victim-support organisations went further and argued strongly for the need for victims' voices to be heard independently. The NSPCC in particular made a very powerful argument for children's voices needing to be heard and for having independent advocacy. There would be a significant issue with trust levels if we were to rely solely on the platforms themselves to provide such victim support.

There are a couple of other reasons why we need the Government to tease the issue out. We are talking about the most significant culture change imaginable for the online platforms to go through. There will be a lot of good will, I am sure, to achieve that culture change, but there will also be problems along the way. Again referring back to our evidence sessions, the charity Refuge said that reporting systems are "not up to scratch" currently. There is a lot of room for change. We know that Revenge Porn Helpline has seen a continual increase in demand for its services in support of victims, in particular following the pandemic. It also finds revenue and funding a little hand to mouth.

Victim support organisations will have a crucial role in assisting Ofcom with the elements outlined in chapter 6, of which clause 110 is the start, in terms of monitoring the reality for users of how the platforms are performing. The "polluter pays" principle is not working quite as the Government might want it to in the Bill. My solution is for the Minister to consider talking to his colleagues in the Treasury about whether this circle could be squared—whether we could complete the circle—by having some sort of hypothecation of the financial penalties, so that some of the huge amount that will be levied in penalties can be put into a fund that can be used directly to support victims' organisations. I know that that requires the Department for Digital, Culture, Media and Sport and the Ministry of Justice to work together, but my hon. Friend is incredibly good at collaborative working, and I am sure he will be able to achieve that.

This is not an easy thing. I know that the Treasury would not welcome Committees such as this deciding how financial penalties are to be used, but this is not typical legislation. We are talking about enormous amounts of money and enormous numbers of victims, as the Minister himself has set out when we have tried to debate some of these issues. He could perhaps undertake to raise this issue directly with the Treasury, and perhaps get it to look at how much money is currently going to organisations to support victims of online abuse and online fraud—the list goes on—and to see whether we will have to take a different approach to ensure that the victims we are now recognising get the support he and his ministerial colleagues want to see.

Chris Philp: First, on the substance of the clause, as the shadow Minister said, the process of providing a provisional notice of contravention gives the subject company a fair chance to respond and put its case, before the full enforcement powers are brought down on its head, and that is of course only reasonable, given how strong and severe these powers are. I am glad there is once again agreement between the two parties.

I would like to turn now to the points raised by my right hon. Friend the Member for Basingstoke, who, as ever, has made a very thoughtful contribution to our proceedings. Let me start by answering her question as to what the Bill says about where fines that are levied will go. We can discover the answer to that question in paragraph 8 of schedule 12, which appears at the bottom of page 206 and the top of page 207—in the unlikely event that Members had not memorised that. If they look at that provision, they will see that the Bill as drafted provides that fines that are levied under the powers provided in it and that are paid to Ofcom get paid over to the Consolidated Fund, which is essentially general Treasury resources. That is where the money goes under the Bill as drafted.

My right hon. Friend asks whether some of the funds could be, essentially, hypothecated and diverted directly to pay victims. At the moment, the Government are dealing with victims, or pay for services supporting victims, not just via legislation—the victims Bill—but via expenditure that, I think, is managed by the Ministry of Justice to support victims and organisations working with victims in a number of ways. I believe that the amount earmarked for this financial year is in excess of £300 million, which is funded just via the general spending review. That is the situation as it is today.

I am happy to ask colleagues in Government the question that my right hon. Friend raises. It is really a matter for the Treasury, so I am happy to pass her idea on to it. But I anticipate a couple of responses coming

[Chris Philp]

from the Treasury in return. I would anticipate it first saying that allocating money to a particular purpose, including victims, is something that it likes to do via spending reviews, where it can balance all the demands on Government revenue, viewed in the round.

Secondly, it might say that the fine income is very uncertain; we do not know what it will be. One year it could be nothing; the next year it could be billions and billions of pounds. It depends on the behaviour of these social media firms. In fact, if the Bill does its job and they comply with the duties as we want and expect them to, the fines could be zero, because the firms do what they are supposed to. Conversely, if they misbehave, as they have been doing until now, the fines could be enormous. If we rely on hypothecation of these fines as a source for funding victim services, it might be that, in a particular year, we discover that there is no income, because no fines have been levied.

2.45 pm

I was anticipating the Treasury's response as I made those points to the Committee, but since my right hon. Friend spoke with such eloquence, and given her great experience in Government, I shall put her idea to Treasury colleagues. I will happily revert to her when its response is forthcoming, although I have tried to anticipate a couple of points that the Treasury might make.

Question put and agreed to.

Clause 110 accordingly ordered to stand part of the Bill.

Clause 111

REQUIREMENTS ENFORCEABLE BY OFCOM AGAINST PROVIDERS OF REGULATED SERVICES

Alex Davies-Jones: I beg to move amendment 53, in clause 111, page 94, line 24, at end insert—

"Section 136(7C) Code of practice on access to data"

This amendment is linked to Amendment 52.

The Chair: With this it will be convenient to discuss amendment 52, in clause 136, page 118, line 6, at end insert—

"(7A) Following the publication of the report, OFCOM must produce a code of practice on access to data setting out measures with which regulated services are required to comply.

(7B) The code of practice must set out steps regulated services are required to take to facilitate access to date by persons carrying out independent research.

(7C) Regulated services must comply with any measures in the code of practice."

This amendment would require Ofcom to produce a code of practice on access to data.

Alex Davies-Jones: Labour welcomes this important clause, which lists the enforceable requirements. Failure to comply with those requirements can trigger enforcement action. However, the provisions could go further, so we urge the Minister to consider our important amendments.

Amendments 52 and 53 make it abundantly clear that more access to, and availability of, data and information about systems and processes would improve understanding of the online environment. We cannot rely solely on Ofcom to act as problems arise, when new issues could be spotted early by experts elsewhere. The entire regime depends on how bright a light we can shine into the black box of the tech companies, but only minimal data can be accessed.

The amendments would require Ofcom simply to produce a code of practice on access to data. We have already heard that without independent researchers accessing data on relevant harm, the platforms have no real accountability for how they tackle online harms. Civil society and researchers work hard to identify online harms from limited data sources, which can be taken away by the platforms if they choose. Labour feels that the Bill must require platforms, in a timely manner, to share data with pre-vetted independent researchers and academics. The EU's Digital Services Act does that, so will the Minister confirm why such a provision is missing from this supposed world-leading Bill?

Clause 136 gives Ofcom two years to assess whether access to data is required, and it "may", but not "must", publish guidance on how its approach to data access might work. The process is far too slow and, ultimately, puts the UK behind the EU, whose legislation makes data access requests possible immediately. Amendment 52 would change the "may" to "must", and would ultimately require Ofcom to explore how access to data works, not if it should happen in the first place.

Kirsty Blackman: Frances Haugen's evidence highlighted quite how shadowy a significant number of the platforms are. Does the hon. Member agree that that hammers home the need for independent researchers to access as much detail as possible so that we can ensure that the Bill is working?

Alex Davies-Jones: I agree 100%. The testimony of Frances Haugen, the Facebook whistleblower, highlighted the fact that expert researchers and academics will need to examine the data and look at what is happening behind social media platforms if we are to ensure that the Bill is truly fit for purpose and world leading. That process should be carried out as quickly as possible, and Ofcom must also be encouraged to publish guidance on how access to data will work.

Ultimately, the amendments make a simple point: civil society and researchers should be able to access data, so why will the Minister not let them? The Bill should empower independently verified researchers and civil society to request tech companies' data. Ofcom should be required to publish guidance as soon as possible —within months, not years—on how data may be accessed. That safety check would hold companies to account and make the internet a safer and less divisive space for everyone.

The process would not be hard or commercially ruinous, as the platforms claim. The EU has already implemented it through its Digital Services Act, which opens up the secrets of tech companies' data to Governments, academia and civil society in order to protect internet users. If we do not have that data, researchers based in the EU will be ahead of those in the UK. Without more insight to enable policymaking, quality research and harm analysis, regulatory intervention in the UK will stagnate. What is more, without such data, we will not know Instagram's true impact on teen mental health, nor the reality of violence against women and girls online or the risks to our national security.

We propose amending the Bill to accelerate data sharing provisions while mandating Ofcom to produce guidance on how civil society and researchers can access data, not just on whether they should. As I said, that should happen within months, not years. The provisions should be followed by a code of practice, as outlined in the amendment, to ensure that platforms do not duck and dive in their adherence to transparency requirements. A code of practice would help to standardise data sharing in a way that serves platforms and researchers.

The changes would mean that tech companies can no longer hide in the shadows. As Frances Haugen said of the platforms in her evidence a few weeks ago:

"The idea that they have worked in close co-operation with researchers is a farce. The only way that they are going to give us even the most basic data that we need to keep ourselves safe is if it is mandated in the Bill. We need to not wait two years after the Bill passes".—[*Official Report, Online Safety Public Bill Committee,* 26 May 2022; c. 188, Q320.]

Chris Philp: I understand the shadow Minister's point. We all heard from Frances Haugen about the social media firms' well-documented reluctance—to put it politely—to open themselves up to external scrutiny. Making that happen is a shared objective. We have already discussed several times the transparency obligations enshrined in clause 64. Those will have a huge impact in ensuring that the social media firms open up a lot more and become more transparent. That will not be an option; they will be compelled to do that. Ofcom is obliged under clause 64 to publish the guidance around those transparency reports. That is all set in train already, and it will be extremely welcome.

Researchers' access to information is covered in clause 136, which the amendments seek to amend. As the shadow Minister said, our approach is first to get Ofcom to prepare a report into how that can best be done. There are some non-trivial considerations to do with personal privacy and protecting people's personal information, and there are questions about who counts as a valid researcher. When just talking about it casually, it might appear obvious who is or is not a valid researcher, but we will need to come up with a proper definition of "valid researcher" and what confidentiality obligations may apply to them.

Barbara Keeley (Worsley and Eccles South) (Lab): This is all sorted in the health environment because of the personal data involved—there is no data more personal than health data—and a trusted and safe environment has been created for researchers to access personal data.

Chris Philp: This data is a little different—the two domains do not directly correspond. In the health area, there has been litigation—an artificial intelligence company is currently engaged in litigation with an NHS hospital trust about a purported breach of patient data rules—so even in that long-established area, there is uncertainty and recent, or perhaps even current, litigation.

We are asking for the report to be done to ensure that those important issues are properly thought through. Once they are, Ofcom has the power under clause 136 to lay down guidance on providing access for independent researchers to do their work.

Kirsty Blackman: The Minister has committed to Ofcom being fully resourced to do what it needs to do under the Bill, but he has spoken about time constraints. If Ofcom were to receive 25,000 risk assessments, for example, there simply would not be enough people to go through them. Does he agree that, in cases in which Ofcom is struggling to manage the volume of data and to do the level of assessment required, it may be helpful to augment that work with the use of independent researchers? I am not asking him to commit to that, but to consider the benefits.

Chris Philp: Yes, I would agree that bona fide academic independent researchers do have something to offer and to add in this area. The more we have highly intelligent, experienced and creative people looking at a particular problem or issue, the more likely we are to get a good and well-informed result. They may have perspectives that Ofcom does not. I agree that, in principle, independent researchers can add a great deal, but we need to ensure that we get that set up in a thoughtful and proper way. I understand the desire to get it done quickly, but it is important to take the time to do it not just quickly, but right. It is an area that does not exist already—at the moment, there is no concept of independent researchers getting access to the innards of social media companies' data vaults—so we need to make sure that it is done in the right way, which is why it is structured as it is. I ask the Committee to stick with the drafting, whereby there will be a report and then Ofcom will have the power. I hope we end up in the same place—well, the same place, but a better place. The process may be slightly slower, but we may also end up in a better place for the consideration and thought that will have to be given.

Alex Davies-Jones: I appreciate where the Minister is coming from. It seems that he wants to back the amendment, so I am struggling to see why he will not, especially given that the DSA—the EU's new legislation—is already doing this. We know that the current wording in the Bill is far too woolly. If providers can get away with it, they will, which is why we need to compel them, so that we are able to access this data. We need to put that on the face of the Bill. I wish that we did not have to do so, but we all wish that we did not have to have this legislation in the first place. Unless we put it in the Bill, however, the social media platforms will carry on regardless, and the internet will not be a safe place for children and adults in the UK. That is why I will push amendment 53 to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 3, Noes 5.

Division No. 35]

AYES

Blackman, Kirsty	Keeley, Barbara
Davies-Jones, Alex	

NOES

Bailey, Shaun	Philp, Chris
Fletcher, Nick	
Miller, rh Dame Maria	Russell, Dean

Question accordingly negatived.

Alex Davies-Jones: I beg to move amendment 56, in clause 111, page 94, line 24, at end insert—

"Section [Supply chain risk assessment duties]	Supply chain risk assessments"

This amendment is linked to NC11.

The Chair: With this it will be convenient to discuss new clause 11—*Supply chain risk assessment duties*—

"(1) This section sets out duties to assess risks arising in a provider's supply chain, which apply to all Part 3 services.

(2) A duty to carry out a suitable and sufficient assessment of the risk of harm arising to persons employed by contractors of the provider, where the role of such persons is to moderate content on the service.

(3) A duty to keep the risk assessment up to date.

(4) Where any change is proposed to any contract for the moderation of content on the service, a duty to carry out a further suitable and sufficient risk assessment.

(5) In this section, the 'risk of harm' includes any risks arising from—

(a) exposure to harmful content; and

(b) a lack of training, counselling or support."

This new clause introduces a duty to assess the risk of harm in the supply chain.

Alex Davies-Jones: We know that human content moderation is the foundation of all content moderation for major platforms. It is the most important resource for making platforms safe. Relying on AI alone is an ineffective and risky way to moderate content, so platforms have to rely on humans to make judgment calls about context and nuance. I pay tribute to all human moderators for keeping us all safe by having to look at some of the most horrendous and graphic content.

The content moderation reviews carried out by humans, often at impossible speeds, are used to classify content to train algorithms that are then used to automatically moderate exponentially more content. Human moderators can be, and often are, exploited by human resource processes that do not disclose the trauma inherent in the work or properly support them in their dangerous tasks. There is little oversight of this work, as it is done largely through a network of contracted companies that do not disclose their expectations for staff or the support and training provided to them. The contractors are "off book" from the platforms and operate at arm's length from the services they are supporting, and they are hidden by a chain of unaccountable companies. This creates a hazardous supply chain for the safety processes that platforms claim will protect users in the UK and around the world.

Not all online abuse in the UK happens in English, and women of many cultures and backgrounds in the UK are subject to horrific abuse that is not in the English language. The amendment would make all victim groups in the UK much safer.

To make the internet safer it is imperative to better support human content moderators and regulate the supply chain for their work. It is an obvious but overlooked point that content moderators are users of a platform, but they are also the most vulnerable group of users, as they are the frontline of defence in sifting out harmful content. Their sole job is to watch gruesome, traumatising and harmful content so that we do not have to. The Bill has a duty to protect the most vulnerable users, but it cannot do so if their existence is not even acknowledged.

Many reports in the media have described the lack of clarity about, and the exploitative nature of, the hiring process. Just yesterday, I had the immense privilege of meeting Daniel Motaung, the Facebook whistleblower from Kenya who has described the graphic and horrendous content that he was required to watch to keep us all safe, including live beheadings and children being sexually exploited. Members of the Committee cannot even imagine what that man has had to endure, and I commend him for his bravery in speaking out and standing up for his rights. He has also been extremely exploited by Facebook and the third party company by which he was employed. He was paid the equivalent of $2 an hour for doing that work, whereas human moderators in the US were paid roughly $18 an hour—again, nowhere near enough for what they had to endure.

3 pm

In one instance, a Meta content moderator working for a contractor was not informed during his interview that the job would require regular viewing of disturbing content that could lead to mental health problems. After he accepted the role, the contractor asked him to sign a non-disclosure agreement, and only then did they reveal to him the exact type of content that he would be working with daily. That moderator—similar to many moderators in the US, Ireland and other locations—was diagnosed with post-traumatic stress disorder due to his work.

One former counsellor for a content moderator contractor

"witnessed managers repeatedly rejecting content moderators' requests for breaks, citing productivity pressures."

They also reported that managers

"regularly rejected counsellors' requests to let content moderators take 'wellness breaks' during the day, because of the impact it would have on productivity."

Other moderators in the US were allocated just nine minutes a day of "wellness time", which many needed to use to go to the bathroom. In some cases, the wellness coaches that the contractors provide do not have any clinical psychological counselling credentials, and would recommend "karaoke or painting" after shifts of watching suicides and other traumatic content.

Oversight is required to ensure that human resources processes clearly identify the role and provide content descriptions, as well as information on possible occupational hazards. Currently, the conditions of the work are unregulated and rely on the business relationship between two parties focused on the bottom line. Platforms do not release any due diligence on the employment conditions of those contractors, if they conduct it at all. If there is to be any meaningful oversight of the risks inherent in the content moderation supply chain, it is imperative to mandate transparency around the conditions for content moderators in contracted entities. As long as that relationship is self-regulated, the wellness of human moderators will be at risk. That is why we urge the Minister to support this important amendment and new clause: there is a human element to all this. We urge him to do the right thing.

Kirsty Blackman: I thank the hon. Member for Pontypridd for laying out her case in some detail, though nowhere near the level of detail that these people have to experience while providing moderation. She has given a very good explanation of why she is asking for the amendment and new clause to be included in the Bill. Concerns are consistently being raised, particularly by the Labour party, about the impact on the staff members who have to deal with this content.

I do not think the significance of this issue for those individuals can be overstated. If we intend the Bill to have the maximum potential impact and reduce harm to the highest number of people possible, it makes eminent sense to accept this amendment and new clause.

There is a comparison with other areas in which we place similar requirements on other companies. The Government require companies that provide annual reports to undertake an assessment in those reports of whether their supply chain uses child labour or unpaid labour, or whether their factories are safe for people to work in—if they are making clothes, for example. It would not be an overly onerous request if we were to widen those requirements to take account of the fact that so many of these social media companies are subjecting individuals to trauma that results in them experiencing PTSD and having to go through a lengthy recovery process, if they ever recover. We have comparable legislation, and that is not too much for us to ask. Unpaid labour, or people being paid very little in other countries, is not that different from what social media companies are requiring of their moderators, particularly those working outside the UK and the US in countries where there are less stringent rules on working conditions. I cannot see a reason for the Minister to reject the provision of this additional safety for employees who are doing an incredibly important job that we need them to be doing, in circumstances where their employer is not taking any account of their wellbeing.

Barbara Keeley: As my hon. Friend the Member for Pontypridd has pointed out, there is little or no transparency about one of the most critical ways in which platforms tackle harms. Human moderators are on the frontline of protecting children and adults from harmful content. They must be well resourced, trained and supported in order to fulfil that function, or the success of the Bill's aims will be severely undermined.

I find it shocking that platforms offer so little data on human moderation, either because they refuse to publish it or because they do not know it. For example, in evidence to the Home Affairs Committee, William McCants from YouTube could not give precise statistics for its moderator team after being given six days' notice to find the figure, because many moderators were employed or operated under third-party auspices. For YouTube's global counter-terrorism lead to be unaware of the detail of how the platform is protecting its users from illegal content is shocking, but it is not uncommon.

In evidence to this Committee, Meta's Richard Earley was asked how many of Meta's 40,000 human moderators were outsourced to remove illegal content and disinformation from the platform. My hon. Friend the Member for Pontypridd said:

"You do not have the figures, so you cannot tell me."

Richard Earley replied:

"I haven't, no, but I will be happy to let you know afterwards in our written submission."

Today, Meta submitted its written evidence to the Committee. It included no reference to human content moderators, despite its promise.

The account that my hon. Friend gave just now shows why new clause 11 is so necessary. Meta's representative told this Committee in evidence:

"Everyone who is involved in reviewing content at Meta goes through an extremely lengthy training process that lasts multiple weeks, covering not just our community standards in total but also the specific area they are focusing on, such as violence and incitement."—[*Official Report, Online Safety Public Bill Committee,* 24 May 2022; c. 45, Q76.]

But now we know from whistleblowers such as Daniel, whose case my hon. Friend described, that that is untrue. What is happening to Daniel and the other human moderators is deeply concerning. There are powerful examples of the devastating emotional impact that can occur because human moderators are not monitored, trained and supported.

There are risks of platforms shirking responsibility when they outsource moderation to third parties. Stakeholders have raised concerns that a regulated company could argue that an element of its service is not in the scope of the regulator because it is part of a supply chain. We will return to that issue when we debate new clause 13, which seeks to ensure enforcement of liability for supply chain failures that amount to a breach of one of the specified duties.

Platforms, in particular those supporting user-to-user generated content, employ those services from third parties. Yesterday, I met Danny Stone, the chief executive of the Antisemitism Policy Trust, who described the problem of antisemitic GIFs. Twitter would say, "We don't supply GIFs. The responsibility is with GIPHY." GIPHY, as part of the supply chain, would say, "We are not a user-to-user platform." If someone searched Google for antisemitic GIFs, the results would contain multiple entries saying, "Antisemitic GIFs—get the best GIFs on GIPHY. Explore and share the best antisemitic GIFs."

One can well imagine a scenario in which a company captured by the regulatory regime established by the Bill argues that an element of its service is not within the ambit of the regulator because it is part of a supply chain presented by, but not necessarily the responsibility of, the regulated service. The contracted element, which I have just described by reference to Twitter and GIPHY, supported by an entirely separate company, would argue that it was providing a business-to-business service that is not user-generated content but content designed and delivered at arm's length and provided to the user-to-user service to deploy for its users.

I suggest that dealing with this issue would involve a timely, costly and unhelpful legal process during which systems were not being effectively regulated—the same may apply in relation to moderators and what my hon. Friend the Member for Pontypridd described; there are a number of lawsuits involved in Daniel's case—and complex contract law was invoked.

We recognise in UK legislation that there are concerns and issues surrounding supply chains. Under the Bribery Act 2010, for example, a company is liable if anyone performing services for or on the company's behalf is found culpable for specific actions. These issues on supply chain liability must be resolved if the Bill is to fulfil its aim of protecting adults and children from harm.

Chris Philp: May I first say a brief word about clause stand part, Sir Roger?

The Chair: Yes.

Chris Philp: Thank you. Clause 111 sets out and defines the "enforceable requirements" in this chapter—the duties that Ofcom is able to enforce against. Those are set out clearly in the table at subsection (2) and the requirements listed in subsection (3).

The amendment speaks to a different topic. It seeks to impose or police standards for people employed as subcontractors of the various companies that are in scope of the Bill, for example people that Facebook contracts; the shadow Minister, the hon. Member for Pontypridd, gave the example of the gentleman from Kenya she met yesterday. I understand the point she makes and I accept that there are people in those supply chains who are not well treated, who suffer PTSD and who have to do extraordinarily difficult tasks. I do not dispute at all the problems she has referenced. However, the Government do not feel that the Bill is the right place to address those issues, for a couple of reasons.

First, in relation to people who are employed in the UK, we have existing UK employment and health and safety laws. We do not want to duplicate or cut across those. I realise that they relate only to people employed in the UK, but if we passed the amendment as drafted, it would apply to people in the UK as much as it would apply to people in Kenya.

Secondly, the amendment would effectively require Ofcom to start paying regard to employment conditions in Kenya, among other places—indeed, potentially any country in the world—and it is fair to say that that sits substantially outside Ofcom's area of expertise as a telecoms and communications regulator. That is the second reason why the amendment is problematic.

The third reason is more one of principle. The purpose of the Bill is to keep users safe online. While I understand the reasonable premise for the amendment, it seeks essentially to regulate working conditions in potentially any country in the world. I am just not sure that it is appropriate for an online safety Bill to seek to regulate global working conditions. Facebook, a US company, was referenced, but only 10% of its activity—very roughly speaking—is in the UK. The shadow Minister gave the example of Kenyan subcontractors. Compelling though her case was, I am not sure it is appropriate that UK legislation on online safety should seek to regulate the Kenyan subcontractor of a United States company.

The Government of Kenya can set their own employment regulations and President Biden's Government can impose obligations on American companies. For us, via a UK online safety Bill, to seek to regulate working conditions in Kenya goes a long way beyond the bounds of what we are trying to do, particularly when we take into account that Ofcom is a telecommunications and communications regulator. To expect it to regulate working conditions anywhere in the world is asking quite a lot.

I accept that a real issue is being raised. There is definitely a problem, and the shadow Minister and the hon. Member for Aberdeen North are right to raise it, but for the three principal reasons that I set out, I suggest that the Bill is not the place to address these important issues.

Alex Davies-Jones: The Minister mentions workers in the UK. I am a proud member of the Labour party and a proud trade unionist; we have strong protections for workers in the UK. There is a reason why Facebook and some of these other platforms, which are incredibly exploitative, will not have human moderators in the UK looking at this content: because they know they would be compelled to treat them a hell of a lot better than they do the workers around the world that they are exploiting, as they do in Kenya, Dublin and the US.

To me, the amendment speaks to the heart of the Bill. This is an online safety Bill that aims to keep the most vulnerable users safe online. People around the world are looking at content that is created here in the UK and having to moderate it; we are effectively shipping our trash to other countries and other people to deal with it. That is not acceptable. We have the opportunity here to keep everybody safe from looking at this incredibly harmful content. We have a duty to protect those who are looking at content created in the UK in order to keep us safe. We cannot let those people down. The amendment and new clause 11 give us the opportunity to do that. We want to make the Bill world leading. We want the UK to stand up for those people. I urge the Minister to do the right thing and back the amendment.

3.15 pm

Barbara Keeley: The Minister has not commented on the problem I raised of the contracted firm in the supply chain not being covered by the regulations under the Bill—the problem of Twitter and the GIFs, whereby the GIFs exist and are used on Twitter, but Twitter says, "We're not responsible for them; it's that firm over there." That is the same thing, and new clause 11 would cover both.

Chris Philp: I am answering slightly off the cuff, but I think the point the hon. Lady is raising—about where some potentially offensive or illegal content is produced on one service and then propagated or made available by another—is one we debated a few days ago. I think the hon. Member for Aberdeen North raised that question, last week or possibly the week before. I cannot immediately turn to the relevant clause—it will be in our early discussions in *Hansard* about the beginning of the Bill—but I think the Bill makes it clear that where content is accessed through another platform, which is the example that the hon. Member for Worsley and Eccles South just gave, the platform through which the content is made available is within the scope of the Bill.

Question put, That the amendment be made.

The Committee divided: Ayes 3, Noes 4.

Division No. 36]

AYES

Blackman, Kirsty	Keeley, Barbara
Davies-Jones, Alex	

NOES

Bailey, Shaun	Philp, Chris
Miller, rh Dame Maria	Russell, Dean

Question accordingly negatived.

Clause 111 ordered to stand part of the Bill.

Clause 112

CONFIRMATION DECISIONS

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

The Chair: With this it will be convenient to discuss clauses 113 to 117 stand part.

Alex Davies-Jones: We support clause 112, which gives Ofcom the power to issue a confirmation decision if, having followed the required process—for example, in clause 110—its final decision is that a regulated service has breached an enforceable requirement. As we know, this will set out Ofcom's final decision and explain whether Ofcom requires the recipient of the notice to take any specific steps and/or pay a financial penalty. Labour believes that this level of scrutiny and accountability is vital to an Online Safety Bill that is truly fit for purpose, and we support clause 112 in its entirety.

We also support the principles of clause 113, which outlines the steps that a person may be required to take either to come into compliance or to remedy the breach that has been committed. Subsection (5) in particular is vital, as it outlines how Ofcom can require immediate action when the breach has involved an information duty. We hope this will be a positive step forward in ensuring true accountability of big tech companies, so we are happy to support the clause unamended.

It is right and proper that Ofcom has powers when a regulated provider has failed to carry out an illegal content or children's risk assessment properly or at all, and when it has identified a risk of serious harm that the regulated provider is not effectively mitigating or managing. As we have repeatedly heard, risk assessments are the very backbone of the Bill, so it is right and proper that Ofcom is able to force a company to take measures to comply in the event of previously failing to act.

Children's access assessments, which are covered by clause 115, are a crucial component of the Bill. Where Ofcom finds that a regulated provider has failed to properly carry out an assessment, it is vital that it has the power and legislative standing to force the company to do more. We also appreciate the inclusion of a three-month timeframe, which would ensure that, in the event of a provider re-doing the assessment, it would at least be completed within a specific—and small—timeframe.

While we recognise that the use of proactive technologies may come with small issues, Labour ultimately feels that clause 116 is balanced and fair, as it establishes that Ofcom may require the use of proactive technology only on content that is communicated publicly. It is fair that content in the public domain is subject to those important safety checks. It is also right that under subsection (7), Ofcom may set a requirement forcing services to review the kind of technology being used. That is a welcome step that will ensure that platforms face a level of scrutiny that has certainly been missing so far.

Labour welcomes and is pleased to support clause 117, which allows Ofcom to impose financial penalties in its confirmation decision. That is something that Labour has long called for, as we believe that financial penalties of this nature will go some way towards improving best practice in the online space and deterring bad actors more widely.

Chris Philp: The shadow Minister has set out the provisions in the clauses, and I am grateful for her support. In essence, clauses 112 to 117 set out the processes around confirmation decisions and make provisions to ensure that those are effective and can be operated in a reasonable and fair way. The clauses speak largely for themselves, so I am not sure that I have anything substantive to add.

Question put and agreed to.

Clause 112 accordingly ordered to stand part of the Bill.

Clauses 113 to 117 ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned. *—(Dean Russell.)*

3.21 pm

Adjourned till Tuesday 21 June at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

OSB77 Twitter