PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

ONLINE SAFETY BILL

Fifth Sitting

Tuesday 7 June 2022

(Morning)

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

(Morning)

[Sir Roger Gale *in the Chair*]

Online Safety Bill

9.25 am

The Chair: Good morning, ladies and gentleman. If anybody wishes to take their jacket off, they are at liberty to do so when I am in the Chair—my co-Chairman is joining us, and I am sure she will adopt the same procedure. I have a couple of preliminary announcements. Please make sure that all mobile phones are switched off. Tea and coffee are not allowed in the Committee, I am afraid. I think they used to be available outside in the corridor, but I do not know whether that is still the case.

We now start line-by-line consideration of the Bill. The selection and grouping list for the sitting is available on the table in the room for anybody who does not have it. It shows how the clauses and selected amendments have been grouped for debate. Grouped amendments are generally on the same subject or a similar issue.

Now for a slight tutorial to remind me and anybody else who is interested, including anybody who perhaps has not engaged in this arcane procedure before, of the proceedings. Each group has a lead amendment, and that amendment is moved first. The other grouped amendments may be moved later, but they are not necessarily voted on at that point, because some of them relate to matters that appear later in the Bill. Do not panic; that does not mean that we have forgotten them, but that we will vote on them—if anybody wants to press them to a Division—when they are reached in order in the Bill. However, if you are in any doubt and feel that we have missed something—occasionally I do; the Clerks never do—just let us know. I am relaxed about this, so if anybody wants to ask a question about anything that they do not understand, please interrupt and ask, and we will endeavour to confuse you further.

The Member who has put their name to the lead amendment, and only the lead amendment, is usually called to speak first. At the end of the debate, the Minister will wind up, and the mover of the lead amendment—that might be the Minister if it is a Government amendment, or it might be an Opposition Member—will indicate whether they want a vote on that amendment. We deal with that first, then we deal with everything else in the order in which it arises. I hope all that is clear, but as I said, if there are any questions, please interrupt and ask.

We start consideration of the Bill with clause 1, to which there are no amendments. Usually, the Minister would wind up at the end of each debate, but as there are no amendments to clause 1, the Minister has indicated that he would like to say a few words about the clause.

Clause 1

Overview of Act

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

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Chris Philp): Thank you, Sir Roger; it is a pleasure to serve under your chairmanship once again. It may be appropriate to take this opportunity to congratulate my right hon. Friend the Member for Basingstoke on her damehood in the Queen's birthday honours, which was very well deserved indeed.

This simple clause provides a high-level overview of the different parts of the Bill and how they come together to form the legislation.

The Chair: The Minister was completely out of order in congratulating the right hon. Lady, but I concur with him. I call the shadow Minister.

Alex Davies-Jones (Pontypridd) (Lab): Thank you, Sir Roger; it is a genuine privilege and an honour to serve under your chairship today and for the duration of the Committee. I concur with congratulations to the right hon. Member for Basingstoke and I, too, congratulate her.

If you would indulge me, Sir Roger, this is the first time I have led on behalf of the Opposition in a Bill Committee of this magnitude. I am very much looking forward to getting my teeth stuck into the hours of important debate that we have ahead of us. I would also like to take this opportunity to place on record an early apology for any slight procedural errors I may inadvertently make as we proceed. However, I am very grateful to be joined by my hon. Friend the Member for Worsley and Eccles South, who is much more experienced in these matters. I place on record my grateful support to her. Along with your guidance, Sir Roger, I expect that I will quickly pick up the correct parliamentary procedure as we make our way through this colossal legislation. After all, we can agree that it is a very important piece of legislation that we all need to get right.

I want to say clearly that the Opposition welcome the Bill in principle; the Minister knows that, as we voted in favour of it at Second Reading. However, it will come as no surprise that we have a number of concerns about areas where we feel the Bill is lacking, which we will explore further. We have many reservations about how the Bill has been drafted. The structure and drafting pushes services into addressing harmful content—often in a reactive, rather than proactive, way—instead of harmful systems, business models and algorithms, which would be a more lasting and systemic approach.

Despite that, we all want the Bill to work and we know that it has the potential to go far. We also recognise that the world is watching, so the Opposition look forward to working together to do the right thing, making the internet a truly safe space for all users across the UK. We will therefore not oppose clause 1.

Dan Carden (Liverpool, Walton) (Lab): It is a pleasure to serve on the Committee. I want to apologise for missing the evidence sessions. Unfortunately, I came down with covid, but I have been following the progress of the Committee.

This is important legislation. We spend so much of our lives online these days, yet there has never been an attempt to regulate the space, or for democratically elected Members to contribute towards its regulation. Clause 1 gives a general outline of what to expect in the Bill. I have no doubt that this legislation is required, but also that it will not get everything right, and that it will have to change over the years. We may see many more Bills of this nature in this place.

I have concerns that some clauses have been dropped, and I hope that there will be future opportunities to amend the Bill, not least with regard to how we educate and ensure that social media companies promote media literacy, so that information that is spread widely online is understood in its context—that it is not always correct or truthful. The Bill, I hope, will go some way towards ensuring that we can rely more on the internet, which should provide a safer space for all its users.

Dame Maria Miller (Basingstoke) (Con): May I join others in welcoming line-by-line scrutiny of the Bill? I am sure that the Minister will urge us to ensure that we do not make the perfect the enemy of the good. This is a very lengthy and complex Bill, and a great deal of time and scrutiny has already gone into it. I am sure that we will all pay due regard to that excellent work.

The hon. Member for Pontypridd is absolutely right to say that in many ways the world is watching what the Government are doing regarding online regulation. This will set a framework for many countries around the world, and we must get it right. We are ending the myth that social media and search engines are not responsible for their content. Their use of algorithms alone demonstrates that, while they may not publish all of the information on their sites, they are the editors at the very least and must take responsibility.

We will no doubt hear many arguments about the importance of free speech during these debates and others. I would like gently to remind people that there are many who feel that their free speech is currently undermined by the way in which the online world operates. Women are subject to harassment and worse online, and children are accessing inappropriate material. There are a number of areas that require specific further debate, particularly around the safeguarding of children, adequate support for victims, ensuring that the criminal law is future-proof within this framework, and ensuring that we pick up on the comments made in the evidence sessions regarding the importance of guidance and codes of practice. It was slightly shocking to hear from some of those giving evidence that the operators did not know what was harmful, as much has been written about the harm caused by the internet.

I will listen keenly to the Minister's responses on guidance and codes of practice, and secondary legislation more generally, because it is critical to how the Bill works. I am sure we will have many hours of interesting and informed debate on this piece of legislation. While there has already been a great deal of scrutiny, the Committee's role is pivotal to ensure that the Bill is as good as it can be.

Question put and agreed to.

Clause 1 accordingly ordered to stand part of the Bill.

Clause 2

KEY DEFINITIONS

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

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

Clause 3 stand part.

That schedules 1 and 2 be the First and Second schedules to the Bill.

Clause 4 stand part.

Alex Davies-Jones: We do not oppose clauses 2, 3 or 4, or the intentions of schedules 1 and 2, and have not sought to amend them at this stage, but this is an important opportunity to place on record some of the Opposition's concerns as the Bill proceeds.

The first important thing to note is the broadness in the drafting of all the definitions. A service has links to the UK if it has a significant number of users in the UK, if the UK users are a target market, or if

"there are reasonable grounds to believe there is a material risk of significant harm to individuals"

in the UK using the service. Thus, territorially, a very wide range of online services could be caught. The Government have estimated in their impact assessment that 25,100 platforms will be in scope of the new regime, which is perhaps a conservative estimate. The impact assessment also notes that approximately 180,000 platforms could potentially be considered in scope of the Bill.

The provisions on extraterritorial jurisdiction are, again, extremely broad and could lead to some international platforms seeking to block UK users in a way similar to that seen following the introduction of GDPR. Furthermore, as has been the case under GDPR, those potentially in scope through the extraterritorial provisions may vigorously resist attempts to assert jurisdiction.

Notably absent from schedule 1 is an attempt to include or define how the Bill and its definitions of services that are exempt may adapt to emerging future technologies. The Minister may consider that a matter for secondary legislation, but as he knows, the Opposition feel that the Bill already leaves too many important matters to be determined at a later stage via statutory instruments. Although it good to see that the Bill has incorporated everyday internet behaviour such as a like or dislike button, as well as factoring in the use of emojis and symbols, it fails to consider how technologies such as artificial intelligence will sit within the framework as it stands.

It is quite right that there are exemptions for everyday user-to-user services such as email, SMS, and MMS services, and an all-important balance to strike between our fundamental right to privacy and keeping people safe online. That is where some difficult questions arise on platforms such as WhatsApp, which are embedded with end-to-end encryption as a standard feature. Concerns have been raised about Meta's need to extend that feature to Instagram and Facebook Messenger.

The Opposition also have concerns about private messaging features more widely. Research from the Centre for Missing and Exploited Children highlighted the fact that a significant majority of online child abuse takes place in private messages. For example, 12 million of the 18.4 million child sexual abuse reports made by Facebook in 2019 related to content shared on private

[Alex Davies-Jones]

channels. Furthermore, recent data from the Office for National Statistics shows that private messaging plays a central role in contact between children and people they have not met offline before. Nearly three quarters—74%—of cases of children contacted by someone they do not know initially take place by private message. We will address this issue further in new clause 20, but I wanted to highlight those exemptions early on, as they are relevant to schedule 1.

On a similar point, we remain concerned about how emerging online systems such as the metaverse have had no consideration in Bill as it stands. Only last week, colleagues will have read about a researcher from a non-profit organisation that seeks to limit the power of large corporations, SumOfUs, who claimed that she experienced sexual assault by a stranger in Meta's virtual reality space, Horizon Worlds. The organisation's report said:

"About an hour into using the platform, a SumOfUs researcher was led into a private room at a party where she was raped by a user who kept telling her to turn around so he could do it from behind while users outside the window could see—all while another user in the room watched and passed around a vodka bottle."

There is currently no clear distinction about how these very real technologies will sit in the Bill more widely. Even more worryingly, there has been no consideration of how artificial intelligence systems such as Horizon Worlds, with clear user-to-user functions, fit within the exemptions in schedule 1. If we are to see exemptions for internal business services or services provided by public bodies, along with many others, as outlined in the schedule, we need to make sure that the exemptions are fit for purpose and in line with the rapidly evolving technology that is widely available overseas. Before long, I am sure that reality spaces such as Horizon Worlds will become more and more commonplace in the UK too.

I hope that the Minister can reassure us all of his plans to ensure that the Bill is adequately future-proofed to cope with the rising expansion of the online space. Although we do not formally oppose the provisions outlined in schedule 1, I hope that the Minister will see that there is much work to be done to ensure that the Bill is adequately future-proofed to ensure that the current exemptions are applicable to future technologies too.

Turning to schedule 2, the draft Bill was hugely lacking in provisions to tackle pornographic content, so it is a welcome step that we now see some attempts to tackle the rate at which pornographic content is easily accessed by children across the country. As we all know, the draft Bill only covered pornography websites that allow user-generated content such as OnlyFans. I am pleased to see that commercial pornography sites have now been brought within scope. This positive step forward has been made possible thanks to the incredible efforts of campaigning groups, of which there are far too many to mention, and from some of which we took evidence. I pay tribute to them today. Over the years, it is thanks to their persistence that the Government have been forced to take notice and take action.

Once again—I hate to repeat myself—I urge the Minister to consider how far the current definitions outlined in schedule 2 relating to regulated provider pornographic content will go to protect virtual technologies such as those I referred to earlier. We are seeing an increase in all types of pornographic and semi-pornographic content that draws on AI or virtual technology. An obvious example is the now thankfully defunct app that was making the rounds online in 2016 called DeepNude. While available, the app used neural networks to remove clothing from images of women, making them look realistically nude. The ramifications and potential for technology like this to take over the pornographic content space is essentially limitless.

I urge the Minister carefully to keep in mind the future of the online space as we proceed. More specifically, the regulation of pornographic content in the context of keeping children safe is an area where we can all surely get on board. The Opposition have no formal objection at this stage to the provisions outlined in schedule 2.

Kirsty Blackman (Aberdeen North) (SNP): Thank you, Sir Roger, for chairing our sittings. It is a pleasure to be part of this Bill Committee. I have a couple of comments on clause 2 and more generally.

The Opposition spokesperson, the hon. Member for Pontypridd, made some points about making sure that we are future-proofing the Bill. There are some key issues where we need to make sure that we are not going backwards. That particularly includes private messaging. We need to make sure that the ability to use AI to find content that is illegal, involving child sexual abuse for example, in private messages is still included in the way that it is currently and that the Bill does not accidentally bar those very important safeguards from continuing. That is one way in which we need to be clear on the best means to go forward with the Bill.

Future-proofing is important—I absolutely agree that we need to ensure that the Bill either takes into account the metaverse and virtual reality or ensures that provisions can be amended in future to take into account the metaverse, virtual reality and any other emerging technologies that we do not know about and cannot even foresee today. I saw a meme online the other day that was somebody taking a selfie of themselves wearing a mask and it said, "Can you imagine if we had shown somebody this in 1995 and asked them what this was? They wouldn't have had the faintest idea." The internet changes so quickly that we need to ensure that the Bill is future-proofed, but we also need to make sure that it is today-proofed.

I still have concerns, which I raised on Second Reading, about whether the Bill adequately encompasses the online gaming world, where a huge number of children use the internet—and where they should use it—to interact with their friends in a safe way. A lot of online gaming is free from the bullying that can be seen in places such as WhatsApp, Snapchat and Instagram. We need to ensure that those safeguards are included for online gaming. Private messaging is a thing in a significant number of online games, but many people use oral communication—I am thinking of things such as Fortnite and Roblox, which is apparently a safe space, according to Roblox Corporation, but according to many researchers is a place where an awful lot of grooming takes place.

My other question for the Minister—I am not bothered if I do not get an answer today, as I would rather have a proper answer than the Minister try to come up with an answer right at this moment—is about what category the app store and the Google Play store fall into.

9.45 am

Alex Davies-Jones: On a point of order, Sir Roger. The livestream is not working. In the interest of transparency we should pause the Committee while it is fixed so that people can observe.

The Chair: I am reluctant to do that. It is a technical fault and it is clearly undesirable, but I do not think we can suspend the Committee for the sake of a technical problem. Every member of the public who wishes to express an interest in these proceedings is able to be present if they choose to do so. Although I understand the hon. Lady's concern, we have to continue. We will get it fixed as soon as we can.

Kirsty Blackman *rose—*

Kim Leadbeater (Batley and Spen) (Lab): Will the hon. Lady give way?

Kirsty Blackman: Absolutely.

Kim Leadbeater: You are making some really important points about the world of the internet and online gaming for children and young people. That is where we need some serious consideration about obligations on providers about media literacy for both children and grown-ups. Many people with children know that this is a really dangerous space for young people, but we are not quite sure we have enough information to understand what the threats, risks and harms are. That point about media literacy, particularly in regard to the gaming world, is really important.

The Chair: Order. Before we proceed, the same rules apply in Committee as on the Floor of the House to this extent: the Chair is "you", and you speak through the Chair, so it is "the hon. Lady". *[Interruption.]* One moment.

While I am on my feet, I should perhaps have said earlier, and will now say for clarification, that interventions are permitted in exactly the same way as they are on the Floor of the House. In exactly the same way, it is up to the Member who has the Floor to decide whether to give way or not. The difference between these debates and those on the Floor of the House is of course that on the Floor of the House a Member can speak only once, whereas in Committee you have the opportunity to come back and speak again if you choose to do so. Once the Minister is winding up, that is the end of the debate. The Chair would not normally admit, except under exceptional circumstances, any further speech, as opposed to an intervention.

Kirsty Blackman: Thank you, Sir Roger.

I do not want to get sidetracked, but I agree that there is a major parental knowledge gap. Tomorrow's parents will have grown up on the internet, so in 20 years' time we will have not have that knowledge gap, but today media literacy is lacking particularly among parents as well as among children. In Scotland, media literacy is embedded in the curriculum; I am not entirely sure what the system is in the rest of the UK. My children are learning media literacy in school, but there is still a gap about media literacy for parents. My local authority is doing a media literacy training session for parents tomorrow night, which I am very much looking forward to attending so that I can find out even more about how to keep my children safe online.

I was asking the Minister about the App Store and the Google Play Store. I do not need an answer today, but one at some point would be really helpful. Do the App Store, the Google Play Store and other stores of that nature fall under the definition of search engines or of user-to-user content? The reality is that if somebody creates an app, presumably they are a user. Yes, it has to go through an approval process by Apple or Google, but once it is accepted by them, it is not owned by them; it is still owned by the person who generated it. Therefore, are those stores considered search engines, in that they are simply curating content, albeit moderated content, or are they considered user-to-user services?

That is really important, particularly when we are talking about age verification and children being able to access various apps. The stores are the key gateways where children get apps. Once they have an app, they can use all the online services that are available on it, in line with whatever parental controls parents choose to put in place. I would appreciate an answer from the Minister, but he does not need to provide it today. I am happy to receive it at a later time, if that is helpful.

Dame Maria Miller: I want to pick up on two issues, which I hope the Minister can clarify in his comments at the end of this section.

First, when we took evidence, the Internet Watch Foundation underlined the importance of end-to-end encryption being in scope of the Bill, so that it does not lose the ability to pick up child abuse images, as has already been referred to in the debate. The ability to scan end-to-end encryption is crucial. Will the Minister clarify if that is in scope and if the IWF will be able to continue its important work in safeguarding children?

Kirsty Blackman: A number of people have raised concerns about freedom of speech in relation to end-to-end encryption. Does the right hon. Lady agree with me that, there should not be freedom of speech when it comes to child sexual abuse images, and that it is reasonable for those systems to check for child sexual abuse images?

Dame Maria Miller: The hon. Lady is right to pick up on the nuance and the balance that we have to strike in legislation between freedom of speech and the protection of vulnerable individuals and children. I do not think there can be many people, particularly among those here today, who would want anything to trump the safeguarding of children. Will the Minister clarify exactly how the Bill works in relation to such important work?

Secondly, it is important that the Government have made the changes to schedule 2. They have listened closely on the issue of pornography and extended the provisions of the Bill to cover commercial pornography. However, the hon. Member for Pontypridd mentioned nudification software, and I am unclear whether the Bill would outlaw such software, which is designed to sexually harass women. That software takes photographs only of women, because its database relates only to female

[Dame Maria Miller]

figures, and makes them appear to be completely naked. Does that software fall in scope of the Bill? If not, will the Minister do something about that? The software is available and we have to regulate it to ensure that we safeguard women's rights to live without harassment in their day-to-day life.

Dan Carden: This part of the Bill deals with the definitions of services and which services would be exempt. I consider myself a millennial; most people my age or older are Facebook and Twitter users, and people a couple of years younger might use TikTok and other services. The way in which the online space is used by different generations, particularly by young people, changes rapidly. Given the definitions in the Bill, how does the Minister intend to keep pace with the changing ways in which people communicate? Most online games now allow interaction between users in different places, which was not the case a few years ago. Understanding how the Government intend the Bill to keep up with such changes is important. Will the Minister tell us about that?

Chris Philp: Let me briefly speak to the purpose of these clauses and then respond to some of the points made in the debate.

As the shadow Minister, the hon. Member for Pontypridd, touched on, clauses 2 and 3 define some of the key terms in the Bill, including "user-to-user services" and "search services"—key definitions that the rest of the Bill builds on. As she said, schedule 1 and clause 4 contain specific exemptions where we believe the services concerned present very low risk of harm. Schedule 2 sets out exemptions relating to the new duties that apply to commercial providers of pornography. I thank the shadow Minister and my right hon. Friend the Member for Basingstoke for noting the fact that the Government have substantially expanded the scope of the Bill to now include commercial pornography, in response to widespread feedback from Members of Parliament across the House and the various Committees that scrutinised the Bill.

The shadow Minister is quite right to say that the number of platforms to which the Bill applies is very wide. *[Interruption.]* Bless you—or bless my hon. Friend the Member for North West Durham, I should say, Sir Roger, although he is near sanctified already. As I was saying, we are necessarily trying to protect UK users, and with many of these platforms not located in the UK, we are seeking to apply these duties to those companies as well as ones that are domestically located. When we come to discuss the enforcement powers, I hope the Committee will see that those powers are very powerful.

The shadow Minister, the hon. Member for Liverpool, Walton and others asked about future technologies and whether the Bill will accommodate technologies that we cannot even imagine today. The metaverse is a good example: The metaverse did not exist when the Bill was first contemplated and the White Paper produced. Actually, I think Snapchat did not exist when the White Paper that preceded the Bill was first conceived. For that reason, the Bill is tech agnostic. We do not talk about specific technologies; we talk about the duties that apply to companies and the harms they are obligated to prevent.

The whole Bill is tech agnostic because we as parliamentarians today cannot anticipate future developments. When those future developments arise, as they inevitably will, the duties under the Bill will apply to them as well. The metaverse is a good example, because even though it did not exist when the structure of the Bill was conceived, anything happening in the metaverse is none the less covered by the Bill. Anything that happens in the metaverse that is illegal or harmful to children, falls into the category of legal but harmful to adults, or indeed constitutes pornography will be covered because the Bill is tech agnostic. That is an extremely important point to make.

The hon. Member for Aberdeen North asked about gaming. Parents are concerned because lots of children, including quite young children, use games. My own son has started playing Minecraft even though he is very young. To the extent that those games have user-to-user features—for example, user-to-user messaging, particularly where those messages can be sent widely and publicly—those user-to-user components are within the scope of the Bill.

The hon. Member for Aberdeen North also asked about the App Store. I will respond quickly to her question now rather than later, to avoid leaving the Committee in a state of tingling anticipation and suspense. The App Store, or app stores generally, are not in the scope of the Bill, because they are not providing, for example, user-to-user services, and the functionality they provide to basically buy apps does not count as a search service. However, any app that is purchased in an app store, to the extent that it has either search functionality, user-to-user functionality or purveys or conveys pornography, is in scope. If an app that is sold on one of these app stores turns out to provide a service that breaks the terms of the Bill, that app will be subject to regulatory enforcement directly by Ofcom.

The hon. Members for Aberdeen North and for Liverpool, Walton touched on media literacy, noting that there has been a change to the Bill since the previous version. We will probably debate this later, so I will be brief. The Government published a media literacy strategy, backed by funding, to address this point. It was launched about a year ago. Ofcom also has existing statutory duties—arising under the Communications Act 2003, I believe. The critical change made since the previous draft of the Bill—it was made in December last year, I believe—is that Ofcom published an updated set of policy intentions around media literacy that went even further than we had previously intended. That is the landscape around media literacy.

10 am

Dan Carden: On the way that media literacy relates to misinformation and disinformation, we heard from William Moy, chief executive of Full Fact. His view was that the Bill does nothing to tackle disinformation and that another information incident, as we have seen with covid and Ukraine recently, is inevitable. Full Fact's view was that the Bill should give the regulator the power to declare misinformation incidents. Is that something the Minister has considered?

Chris Philp: I am sure we will discuss this topic a bit more as the Bill progresses.

I will make a few points on disinformation. The first is that, non-legislatively, the Government have a counter-disinformation unit, which sits within the Department for Digital, Culture, Media and Sport. It basically scans for disinformation incidents. For the past two years it has been primarily covid-focused, but in the last three or four months it has been primarily Russia/Ukraine-focused. When it identifies disinformation being spread on social media platforms, the unit works actively with the platforms to get it taken down. In the course of the Russia-Ukraine conflict, and as a result of the work of that unit, I have personally called in some of the platforms to complain about the stuff they have left up. I did not have a chance to make this point in the evidence session, but when the person from Twitter came to see us, I said that there was some content on Russian embassy Twitter accounts that, in my view, was blatant disinformation—denial of the atrocities that have been committed in Bucha. Twitter had allowed it to stay up, which I thought was wrong. Twitter often takes down such content, but in that example, wrongly and sadly, it did not. We are doing that work operationally.

Secondly, to the extent that disinformation can cause harm to an individual, which I suspect includes a lot of covid disinformation—drinking bleach is clearly not very good for people—that would fall under the terms of the legal but harmful provisions in the Bill.

Thirdly, when it comes to state-sponsored disinformation of the kind that we know Russia engages in on an industrial scale via the St Petersburg Internet Research Agency and elsewhere, the Home Office has introduced the National Security Bill—in fact, it had its Second Reading yesterday afternoon, when some of us were slightly distracted. One of the provisions in that Bill is a foreign interference offence. It is worth reading, because it is very widely drawn and it criminalises foreign interference, which includes disinformation. I suggest the Committee has a look at the foreign interference offence in the National Security Bill.

Alex Davies-Jones: I am grateful for the Minister's intervention in bringing in the platforms to discuss disinformation put out by hostile nation states. Does he accept that if Russia Today had put out some of that disinformation, the platforms would be unable to take such content down as a result of the journalistic exemption in the Bill?

Chris Philp: We will no doubt discuss in due course clauses 15 and 50, which are the two that I think the shadow Minister alludes to. If a platform is exempt from the duties of the Bill owing to its qualification as a recognised news publisher under clause 50, it removes the obligation to act under the Bill, but it does not prevent action. Social media platforms can still choose to act. Also, it is not a totally straightforward matter to qualify as a regulated news publisher under clause 50. We saw the effect of sanctions: when Russia Today was sanctioned, it was removed from many platforms as a result of the sanctioning process. There are measures outside the Bill, such as sanctions, that can help to address the shocking disinformation that Russia Today was pumping out.

The last point I want to pick up on was rightly raised by my right hon. Friend the Member for Basingstoke and the hon. Member for Aberdeen North. It concerns child sexual exploitation and abuse images, and particularly the ability of platforms to scan for those. Many images are detected as a result of scanning messages, and many paedophiles or potential paedophiles are arrested as a result of that scanning. We saw a terrible situation a little while ago, when—for a limited period, owing to a misconception of privacy laws—Meta, or Facebook, temporarily suspended scanning in the European Union; as a result, loads of images that would otherwise have been intercepted were not.

I agree with the hon. Member for Aberdeen North that privacy concerns, including end-to-end encryption, should not trump the ability of organisations to scan for child sexual exploitation and abuse images. Speaking as a parent—I know she is, too—there is, frankly, nothing more important than protecting children from sexual exploitation and abuse. Some provisions in clause 103 speak to this point, and I am sure we will debate those in more detail when we come to that clause. I mention clause 103 to put down a marker as the place to go for the issue being raised. I trust that I have responded to the points raised in the debate, and I commend the clause to the Committee.

Question put and agreed to.

Clause 2 accordingly ordered to stand part of the Bill.

Clause 3 ordered to stand part of the Bill.

Schedules 1 and 2 agreed to.

Clause 4 ordered to stand part of the Bill.

The Chair: Before we move on, we have raised the issue of the live feed. The audio will be online later today. There is a problem with the feed—it is reaching the broadcasters, but it is not being broadcast at the moment.

As we are not certain we can sort out the technicalities between now and this afternoon, the Committee will move to Committee Room 9 for this afternoon's sitting to ensure that the live stream is available. Mr Double, if Mr Russell intends to be present—he may not; that is up to you—it would be helpful if you would let him know. Ms Blackman, if John Nicolson intends to be present this afternoon, would you please tell him that Committee Room 9 will be used?

It would normally be possible to leave papers and other bits and pieces in the room, because it is usually locked between the morning and afternoon sittings. Clearly, because we are moving rooms, you will all need to take your papers and laptops with you.

Clause 5

Overview of Part 3

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

Alex Davies-Jones: I want to just put it on the record that the irony is not lost on me that we are having tech issues relating to the discussion of the Online Safety Bill. The Opposition have huge concerns regarding clause 5. We share the frustrations of stakeholders who have been working on these important issues for many

[Alex Davies-Jones]

years and who feel the Bill has been drafted in overly complex way. In its evidence, the Carnegie UK Trust outlined its concerns over the complexity of the Bill, which will likely lead to ineffective regulation for both service users and companies. While the Minister is fortunate to have a team of civil servants behind him, he will know that the Opposition sadly do not share the same level of resources—although I would like to place on the record my sincere thanks to my researcher, Freddie Cook, who is an army of one all by herself. Without her support, I would genuinely not know where I was today.

Complexity is an issue that crops up time and again when speaking with charities, stakeholders and civil society. We all recognise that the Bill will have a huge impact however it passes, but the complexity of its drafting is a huge barrier to implementation. The same can be said for the regulation. A Bill as complex as this is likely to lead to ineffective regulation for both service users and companies, who, for the first time, will be subject to specific requirements placed on them by the regulator. That being said, we absolutely support steps to ensure that providers of regulated user-to-user services and regulated search services have to abide by a duty of care regime, which will also see the regulator able to issue codes of practice.

I would also like to place on record my gratitude—lots of gratitude today—to Professor Lorna Woods and Will Perrin, who we heard from in evidence sessions last week. Alongside many others, they have been and continue to be an incredible source of knowledge and guidance for my team and for me as we seek to unpick the detail of this overly complex Bill. Colleagues will also be aware that Professor Woods and Mr Perrin originally developed the idea of a duty of care a few years ago now; their model was based on the idea that social media providers should be,

"seen as responsible for public space they have created, much as property owners or operators are in a physical world."

It will come as no surprise to the Minister that Members of the Opposition fully fall behind that definition and firmly believe that forcing platforms to identify and act on harms that present a reasonable chance of risk is a positive step forward.

More broadly, we welcome moves by the Government to include specific duties on providers of services likely to be accessed by children, although I have some concerns about just how far they will stretch. Similarly, although I am sure we will come to address those matters in the debates that follow, we welcome steps to require Ofcom to issue codes of practice, but have fundamental concerns about how effective they will be if Ofcom is not allowed to remain fully independent and free from Government influence.

Lastly, on subsection 7, I imagine our debate on chapter 7 will be a key focus for Members. I know attempts to define key terms such as "priority content" will be a challenge for the Minister and his officials but we remain concerned that there are important omissions, which we will come to later. It is vital that those key terms are broad enough to encapsulate all the harms that we face online. Ultimately, what is illegal offline must be approached in the same way online if the Bill is to have any meaningful positive impact, which is ultimately what we all want.

Kirsty Blackman: I want to make a couple of brief comments. Unfortunately, my hon. Friend the Member for Ochil and South Perthshire is not here as, ironically, he is at the DCMS committee taking evidence on the Online Safety Bill. That is a pretty unfortunate clash of timing, but that is why I am here solo for the morning.

I wanted to make a quick comment on subsection 7. The Minister will have heard the evidence given on schedule 7 and the fact that the other schedules, particularly schedule 6, has a Scottish-specific section detailing the Scottish legislation that applies. Schedule 7 has no Scotland-specific section and does not adequately cover the Scottish legislation. I appreciate that the Minister has tabled amendment 126, which talks about the Scottish and Northern Irish legislation that may be different from England and Wales legislation, but will he give me some comfort that he does intend Scottish-specific offences to be added to schedule 7 through secondary legislation? There is a difference between an amendment on how to add them and a commitment that they will be added if necessary and if he feels that that will add something to the Bill. If he could commit that that will happen, I would appreciate that—obviously, in discussion with Scottish Ministers if amendment 126 is agreed. It would give me a measure of comfort and would assist, given the oral evidence we heard, in overcoming some of the concerns raised about schedule 7 and the lack of inclusion of Scottish offences.

Dame Maria Miller: In many ways, clause 6 is the central meat of the Bill. It brings into play a duty of care, which means that people operating online will be subject to the same rules as the rest of us when it comes to the provision of services. But when it comes to the detail, the guidance and codes that will be issued by Ofcom will play a central role. My question for the Minister is: in the light of the evidence that we received, I think in panel three, where the providers were unable to define what was harmful because they had not yet seen codes of practice from Ofcom, could he update us on when those codes and guidance might be available? I understand thoroughly why they may not be available at this point, and they certainly should not form part of the Bill because they need to be flexible enough to be changed in future, but it is important that we know how the guidance and codes work and that they work properly.

Will the Minister update the Committee on what further consideration he and other Ministers have given to the establishment of a standing committee to scrutinise the implementation of the Bill? Unless we have that in place, it will be difficult to know whether his legislation will work.

Dan Carden: Some of the evidence we heard suggested that the current precedent was that the Secretary of State had very little to do with independent regulators in this realm, but that the Bill overturns that precedent. Does the right hon. Lady have any concerns that the Bill hands too much power to the Secretary of State to intervene and influence regulators that should be independent?

10.15 am

Dame Maria Miller: The hon. Gentleman brings up an important point. We did hear about that in the evidence. I have no doubt the Secretary of State will not want to interfere in the workings of Ofcom. Having been in his position, I know there would be no desire for the Department to get involved in that, but I can understand why the Government might want the power to ensure things are working as they should. Perhaps the answer to the hon. Gentleman's question is to have a standing committee scrutinising the effectiveness of the legislation and the way in which it is put into practice. That committee could be a further safeguard against what he implies: an unnecessary overreach of the Secretary of State's powers.

Kirsty Blackman: Thank you, Sir Roger, for allowing me to intervene again. I was not expecting the standing committee issue to be brought up at this point, but I agree that there needs to be a post-implementation review of the Bill. I asked a series of written questions to Departments about post-legislative review and whether legislation that the Government have passed has had the intended effect. Most of the Departments that answered could not provide information on the number of post-legislative reviews. Of those that could provide me with the information, none of them had managed to do 100% of the post-implementation reviews that they were supposed to do.

It is important that we know how the Bill's impact will be scrutinised. I do not think it is sufficient for the Government to say, "We will scrutinise it through the normal processes that we normally use," because it is clear that those normal processes do not work. The Government cannot say that legislation they have passed has achieved the intended effect. Some of it will have and some of it will not have, but we do not know because we do not have enough information. We need a standing committee or another way to scrutinise the implementation.

Dame Maria Miller: I thank the hon. Lady for raising this point. Having also chaired a Select Committee, I can understand the sensitivities that this might fall under the current DCMS Committee, but the reality is that the Bill's complexity and other pressures on the DCMS Committee means that this perhaps should be seen as an exceptional circumstance—in no way is that meant as a disrespect to that Select Committee, which is extremely effective in what it does.

Kirsty Blackman: I completely agree. Having sat on several Select Committees, I am aware of the tight timescales. There are not enough hours in the day for Select Committees to do everything that they would like to do. It would be unfortunate and undesirable were this matter to be one that fell between the cracks. Perhaps DCMS will bring forward more legislation in future that could fall between the cracks. If the Minister is willing to commit to a standing committee or anything in excess of the normal governmental procedures for review, that would be a step forward from the position that we are currently in. I look forward to hearing the Minister's views on that.

Dan Carden: I want to add my voice to the calls for ways to monitor the success or failures of this legislation. We are starting from a position of self-regulation where companies write the rules and regulate themselves. It is right that we are improving on that, but with it comes further concerns around the powers of the Secretary of State and the effectiveness of Ofcom. As the issues are fundamental to freedom of speech and expression, and to the protection of vulnerable and young people, will the Minster consider how we better monitor whether the legislation does what it says on the tin?

Chris Philp: Clause 5 simply provides an overview of part 3 of the Bill. Several good points have been raised in the course of this discussion. I will defer replying to the substance of a number of them until we come to the relevant clause, but I will address two or three of them now.

The shadow Minister said that the Bill is a complex, and she is right; it is 193-odd clauses long and a world-leading piece of legislation. The duties that we are imposing on social media firms and internet companies do not already exist; we have no precedent to build on. Most matters on which Parliament legislates have been considered and dealt with before, so we build on an existing body of legislation that has been built up over decades or, in some cases in the criminal law, over centuries. In this case, we are constructing a new legislative edifice from the ground up. Nothing precedes this piece of legislation—we are creating anew—and the task is necessarily complicated by virtue of its novelty. However, I think we have tried to frame the Bill in a way that keeps it as straightforward and as future-proof as possible.

The shadow Minister is right to point to the codes of practice as the source of practical guidance to the public and to social media firms on how the obligations operate in practice. We are working with Ofcom to ensure that those codes of practice are published as quickly as possible and, where possible, prepared in parallel with the passage of the legislation. That is one reason why we have provided £88 million of up-front funding to Ofcom in the current and next financial years: to give it the financial resources to do precisely that.

My officials have just confirmed that my recollection of the Ofcom evidence session on the morning of Tuesday 24 May was correct: Ofcom confirmed to the Committee that it will publish, before the summer, what it described as a "road map" providing details on the timing of when and how those codes of practice will be created. I am sure that Ofcom is listening to our proceedings and will hear the views of the Committee and of the Government. We would like those codes of practice to be prepared and introduced as quickly as possible, and we certainly provided Ofcom with the resources to do precisely that.

There was question about the Scottish offences and, I suppose, about the Northern Irish offences as well—we do not want to forget any part of the United Kingdom.

Alex Davies-Jones: Hear, hear.

Chris Philp: We are in agreement on that. I can confirm that the Government have tabled amendments 116 to 126—the Committee will consider them in due course—to

[Chris Philp]

place equivalent Scottish offences, which the hon. Member for Aberdeen North asked about, in the Bill. We have done that in close consultation with the Scottish Government to ensure that the relevant Scottish offences equivalent to the England and Wales offences are inserted into the Bill. If the Scottish Parliament creates any new Scottish offences that should be inserted into the legislation, that can be done under schedule 7 by way of statutory instrument. I hope that answers the question.

The other question to which I will briefly reply was about parliamentary scrutiny. The Bill already contains a standard mechanism that provides for the Bill to be reviewed after a two to five-year period. That provision appears at the end of the Bill, as we would expect. Of course, there are the usual parliamentary mechanisms—Backbench Business debates, Westminster Hall debates and so on—as well as the DCMS Committee.

I heard the points about a standing Joint Committee. Obviously, I am mindful of the excellent prelegislative scrutiny work done by the previous Joint Committee of the Commons and the Lords. Equally, I am mindful that standing Joint Committees, outside the regular Select Committee structure, unusual. The only two that spring immediately to mind are the Intelligence and Security Committee, which is established by statute, and the Joint Committee on Human Rights, chaired by the right hon. and learned Member for Camberwell and Peckham (Ms Harman), which is established by Standing Orders of the House. I am afraid I am not in a position to make a definitive statement about the Government's position on this. It is of course always open to the House to regulate its own businesses. There is nothing I can say today from a Government point of view, but I know that hon. Members' points have been heard by my colleagues in Government.

We have gone somewhat beyond the scope of clause 5. You have been extremely generous, Sir Roger, in allowing me to respond to such a wide range of points. I commend clause 5 to the Committee.

Question put and agreed to.

Clause 5 accordingly ordered to stand part of the Bill.

Clause 6

PROVIDERS OF USER-TO-USER SERVICES: DUTIES OF CARE

The Chair: Before we proceed, perhaps this is the moment to explain what should happen and what is probably going to happen. Ordinarily, a clause is taken with amendments. This Chairman takes a fairly relaxed view of stand part debates. Sometimes it is convenient to have a very broad-ranging debate on the first group of amendments because it covers matters relating to the whole clause. The Chairman would then normally say, "Well, you've already had your stand part debate, so I'm not going to allow a further stand part debate." It is up to hon. Members to decide whether to confine themselves to the amendment under discussion and then have a further stand part debate, or whether to go free range, in which case the Chairman would almost certainly say, "You can't have a stand part debate as well. You can't have two bites of the cherry."

This is slightly more complex. It is a very complex Bill, and I think I am right in saying that it is the first time in my experience that we are taking other clause stand parts as part of the groups of amendments, because there is an enormous amount of crossover between the clauses. That will make it, for all of us, slightly harder to regulate. It is for that reason—the Minister was kind enough to say that I was reasonably generous in allowing a broad-ranging debate—that I think we are going to have to do that with this group.

I, and I am sure Ms Rees, will not wish to be draconian in seeking to call Members to order if you stray slightly outside the boundaries of a particular amendment. However, we have to get on with this, so please try not to be repetitive if you can possibly avoid it, although I accept that there may well be some cases where it is necessary.

Alex Davies-Jones: I beg to move amendment 69, in clause 6, page 5, line 39, at end insert—

'(6A) All providers of regulated user-to-user services must name an individual whom the provider considers to be a senior manager of the provider, who is designated as the provider's illegal content safety controller, and who is responsible for the provider's compliance with the following duties—

(a) the duties about illegal content risk assessments set out in section 8,

(b) the duties about illegal content set out in section 9.

(6B) An individual is a "senior manager" of a provider if the individual plays a significant role in—

(a) the making of decisions about how the provider's relevant activities are to be managed or organised, or

(b) the actual managing or organising of the provider's relevant activities.

(6C) A provider's "relevant activities" are activities relating to the provider's compliance with the duties of care imposed by this Act.

(6D) The Safety Controller commits an offence if the provider fails to comply with the duties set out in sections 8 and 9 which must be complied with by the provider."

The Chair: With this it will be convenient to discuss amendment 70, in clause 96, page 83, line 7, after "section" insert "6(6D),".

This is one of those cases where the amendment relates to a later clause. While that clause may be debated now, it will not be voted on now. If amendment 69 is negated, amendment 70 will automatically fall later. I hope that is clear, but it will be clearer when we get to amendment 70. Having confused the issue totally, without further ado, I call Ms Davies-Jones.

Alex Davies-Jones: With your permission, Sir Roger, I would like to discuss clause 6 and our amendments 69 and 70, and then I will come back to discuss clauses 7, 21 and 22.

Chapter 2 includes a number of welcome improvements from the draft Bill that the Opposition support. It is only right that, when it comes to addressing illegal content, all platforms, regardless of size or reach, will now be required to develop suitable and sufficient risk assessments that must be renewed before design change is applied. Those risk assessments must be linked to safety duties, which Labour has once again long called for.

It was a huge oversight that, until this point, platforms have not had to perform risk assessments of that nature. During our oral evidence sessions only a few weeks ago, we heard extensive evidence about the range of harms that people face online. Yet the success of the regulatory framework relies on regulated companies carefully assessing the risk posed by their platforms and subsequently developing and implementing appropriate mitigations. Crucial to that, as we will come to later, is transparency. Platforms must be compelled to publish the risk assessments, but in the current version of the Bill, only the regulator will have access to them. Although we welcome the fact that the regulator will have the power to ensure that the risk assessments are of sufficient quality, there remain huge gaps, which I will come on to.

10.30 am

Companies cannot be obligated to act only on risks identified in their own risk assessments, which would surely lead companies to feel compelled to play down the likelihood of current and emerging risks cropping up. Platforms have a track record of burying documents and research that point to risks of harm in their systems and processes. We only have to turn to the revelations we all heard from the incredible Facebook whistleblower, Frances Haugen, about how Facebook—now known as Meta—was failing to tackle global issues such as online human trafficking despite research indicating that its policies were causing direct harm.

Despite that, the Bill should be commended for requiring platforms to document such risks. However, without making those documents public, platforms can continue to hide behind a veil of secrecy. That is why we have tabled a number of amendments to improve transparency measures in the Bill. Under the Bill as drafted, risk assessments will have to be made only to the regulator, and civil society groups, platforms and other interested participants will not have access to them. However, such groups are often at the heart of understanding and monitoring the harms that occur to users online, and they have an in-depth understanding of what mitigations may be appropriate.

We broadly welcome the Government's inclusion of functionality in the risk assessments, which will look at not just content but how it spreads. There remains room for improvement, much of which will be discussed as we delve further into chapter 2.

Our amendment 69 would require regulated companies to designate a senior manager as a safety controller who is legally responsible for ensuring that the service meets its illegality risk assessment and content safety duties and is criminally liable for significant and egregious failures to protect users from harms. Typically, senior executives in technology companies have not taken their safeguarding responsibilities seriously, and Ofcom's enforcement powers remain poorly targeted towards delivering child safety outcomes. The Bill is an opportunity to promote cultural change within companies and to embed compliance with online safety regulations at board level but, as it stands, it completely fails to do so.

Kirsty Blackman: I do not intend to speak to this specific point, but I wholeheartedly agree and will be happy to back amendment 69, should the hon. Lady press it to a vote.

Alex Davies-Jones: I am grateful to the hon. Lady and for SNP support for amendment 69.

The Bill introduces criminal liability for senior managers who fail to comply with information notice provisions, but not for actual failure to fulfil their statutory duties with regard to safety, including child safety, and yet such failures lead to the most seriously harmful outcomes. Legislation should focus the minds of those in leadership positions in services that operate online platforms.

A robust corporate and senior management liability scheme is needed to impose personal liability on directors whose actions consistently and significantly put children at risk. The Bill must learn lessons from other regulated sectors, principally financial services, where regulation imposes specific duties on directors and senior management of financial institutions. Those responsible individuals face regulatory enforcement if they act in breach of such duties. Are we really saying that the financial services sector is more important than child safety online?

The Government rejected the Joint Committee's recommendation that each company appoint a safety controller at, or reporting to, board level. As a result, there is no direct relationship in the Bill between senior management liability and the discharge by a platform of its safety duties. Under the Bill as drafted, a platform could be wholly negligent in its approach to child safety and put children at significant risk of exposure to illegal activity, but as long as the senior manager co-operated with the regulator's investigation, senior managers would not be held personally liable. That is a disgrace.

The Joint Committee on the draft Bill recommended that

"a senior manager at board level or reporting to the board should be designated the 'Safety Controller' and made liable for a new offence: the failure to comply with their obligations as regulated service providers when there is clear evidence of repeated and systemic failings that result in a significant risk of serious harm to users. We believe that this would be a proportionate last resort for the Regulator. Like any offence, it should only be initiated and provable at the end of an exhaustive legal process."

Amendment 69 would make provision for regulated companies to appoint an illegal content safety controller, who has responsibility and accountability for protecting children from illegal content and activity. We believe this measure would drive a more effective culture of online safety awareness within regulated firms by making senior management accountable for harms caused through their platforms and embedding safety within governance structures. The amendment would require consequential amendments setting out the nature of the offences for which the safety officer may be liable and the penalties associated with them.

In financial services regulation, the Financial Conduct Authority uses a range of personal accountability regimes to deter individuals who may exhibit unwanted and harmful behaviour and as mechanisms for bringing about cultural change. The senior managers and certificate regime is an overarching framework for all staff in financial sectors and service industries. It aims to

"encourage a culture of staff at all levels taking personal responsibility for their actions",

and to

"make sure firms and staff clearly understand and can demonstrate where responsibility lies."

Dan Carden: One of the challenges for this legislation will be the way it is enforced. Have my hon. Friend and her Front-Bench colleagues given consideration to the costs of the funding that Ofcom and the regulatory services may need?

Alex Davies-Jones: That is a huge concern for us. As was brought up in our evidence sessions with Ofcom, it is recruiting, effectively, a fundraising officer for the regulator. That throws into question the potential longevity of the regulator's funding and whether it is resourced effectively to properly scrutinise and regulate the online platforms. If that long-term resource is not available, how can the regulator effectively scrutinise and bring enforcement to bear against companies for enabling illegal activity?

Chris Philp: Just to reassure the shadow Minister and her hon. Friend the Member for Liverpool, Walton, the Bill confers powers on Ofcom to levy fees and charges on the sector that it is regulating—so, on social media firms—to recoup its costs. We will debate that in due course—I think it is in clause 71, but that power is in the Bill.

Alex Davies-Jones: I am grateful to the Minister for that clarification and I look forward to debating that further as the Bill progresses.

Returning to the senior managers and certificate regime in the financial services industry, it states that senior managers must be preapproved by the regulator, have their responsibilities set out in a statement of responsibilities and be subject to enhanced conduct standards. Those in banks are also subject to regulatory requirements on their remuneration. Again, it baffles me that we are not asking the same for child safety from online platforms and companies.

The money laundering regulations also use the threat of criminal offences to drive culture change. Individuals can be culpable for failure of processes, as well as for intent. I therefore hope that the Minister will carefully consider the need for the same to apply to our online space to make children safe.

Amendment 70 is a technical amendment that we will be discussing later on in the Bill. However, I am happy to move it in the name of the official Opposition.

The Chair: The Committee will note that, at the moment, the hon. Lady is not moving amendment 70; she is only moving amendment 69. So the Question is, That that amendment be made.

Dan Carden: I congratulate my own Front Bench on this important amendment. I would like the Minister to respond to the issue of transparency and the reason why only the regulator would have sight of these risk assessments. It is fundamental that civil society groups and academics have access to them. Her Majesty's Revenue and Customs is an example of where that works very well. HMRC publishes a lot of its data, which is then used by academics and researchers to produce reports and documents that feed back into the policy making processes and HMRC's work. It would be a missed opportunity if the information and data gathered by Ofcom were not widely available for public scrutiny.

I would reinforce the earlier points about accountability. There are too many examples—whether in the financial crash or the collapse of companies such as Carillion—where accountability was never there. Without this amendment and the ability to hold individuals to account for the failures of companies that are faceless to many people, the legislation risks being absolutely impotent.

Finally, I know that we will get back to the issue of funding in a later clause but I hope that the Minister can reassure the Committee that funding for the enforcement of these regulations will be properly considered.

Chris Philp: Let me start by speaking to clauses 6, 7, 21 and 22 stand part. I will then address the amendments moved by the shadow Minister.

The Chair: Order. I apologise for interrupting, Minister, but the stand part debates on clauses 7, 21 and 22 are part of the next grouping, not this one. I am fairly relaxed about it, but just be aware that you cannot have two debates on this.

Chris Philp: The grouping sheet I have here suggests that clause 7 stand part and clauses 21 and 22 stand part are in this grouping, but if I have misunderstood—

The Chair: No, there are two groups. Let me clarify this for everyone, because it is not as straightforward as it normally is. At the moment we are dealing with amendments 69 and 70. The next grouping, underneath this one on your selection paper, is the clause stand part debates—which is peculiar, as effectively we are having the stand part debate on clause 6 now. For the convenience of the Committee, and if the shadow Minister is happy, I am relaxed about taking all this together.

Alex Davies-Jones: I am happy to come back in and discuss clauses 7, 21 and 22 stand part afterwards.

The Chair: The hon. Lady can be called again. The Minister is not winding up at this point.

Chris Philp: In the interests of simplicity, I will stick to the selection list and adapt my notes accordingly to confine my comments to amendments 69 and 70, and then we will come to the stand part debates in due course. I am happy to comply, Sir Roger.

Speaking of compliance, that brings us to the topic of amendments 69 and 70. It is worth reminding ourselves of the current enforcement provisions in the Bill, which are pretty strong. I can reassure the hon. Member for Liverpool, Walton that the enforcement powers here are far from impotent. They are very potent. As the shadow Minister acknowledged in her remarks, we are for the first time ever introducing senior management liability, which relates to non-compliance with information notices and offences of falsifying, encrypting or destroying information. It will be punishable by a prison sentence of up to two years. That is critical, because without that information, Ofcom is unable to enforce.

We have had examples of large social media firms withholding information and simply paying a large fine. There was a Competition and Markets Authority case a year or two ago where a large social media firm did not provide information repeatedly requested over an extended period and ended up paying a £50 million fine rather than providing the information. Let me put on record now that that behaviour is completely unacceptable. We condemn it unreservedly. It is because we do not want to see that happen again that there will be senior manager criminal liability in relation to providing information, with up to two years in prison.

In addition, for the other duties in the Bill there are penalties that Ofcom can apply for non-compliance. First, there are fines of up to 10% of global revenue. For the very big American social media firms, the UK market is somewhere just below 10% of their global revenue, so 10% of their global revenue is getting on for 100% of their UK revenue. That is a very significant financial penalty, running in some cases into billions of pounds.

In extreme circumstances—if those measures are not enough to ensure compliance—there are what amount to denial of service powers in the Bill, where essentially Ofcom can require internet service providers and others, such as payment providers, to disconnect the companies in the UK so that they cannot operate here. Again, that is a very substantial measure. I hope the hon. Member for Liverpool, Walton would agree that those measures, which are in the Bill already, are all extremely potent.

The question prompted by the amendment is whether we should go further. I have considered that issue as we have been thinking about updating the Bill—as hon. Members can imagine, it is a question that I have been debating internally. The question is whether we should go further and say there is personal criminal liability for breaches of the duties that go beyond information provision. There are arguments in favour, which we have heard, but there are arguments against as well. One is that if we introduce criminal liability for those other duties, that introduces a risk that the social media firms, fearing criminal prosecution, will become over-zealous and just take everything down because they are concerned about being personally liable. That could end up having a chilling effect on content available online and goes beyond what we in Parliament would intend.

10.45 am

Secondly, providing information is pretty cut and dried. We say, "Give us that information. Have you provided it—yes or no? Is that information accurate—yes or no?" It is pretty obvious what the individual executive must do to meet that duty. When it comes to some of the other duties, that clarity that comes with information provision is sometimes less obvious, which makes it harder to justify expanding criminal liability to those circumstances.

Kirsty Blackman: Will the Minister give way?

Chris Philp: In a moment.

For those reasons, I think we have drawn the line in the right place. There is personal criminal liability for information provision, with fines of 10% of local revenue and service disruption—unplugging powers—as well. Having thought about it quite carefully, I think we have struck the balance in the right place. We do not want to deter people from offering services in the UK. If they worried that they might go to prison too readily, it might deter people from locating here. I fully recognise that there is a balance to strike. I feel that the balance is being struck in the right place.

I will go on to comment on a couple of examples we heard about Carillion and the financial crisis, but before I do so, I will give way as promised.

Kirsty Blackman: I appreciate that the Minister says he has been swithering on this point—he has been trying to work out the correct place to draw the line. Given that we do not yet have a commitment for a standing committee—again, that is potentially being considered—we do not know how the legislation is going to work. Will the Minister, rather than accepting the amendment, give consideration to including the ability to make changes via secondary legislation so that there is individual criminal liability for different breaches? That would allow him the flexibility in the future, if the regime is not working appropriately, to add through secondary legislation individual criminal liability for breaches beyond those that are currently covered.

Chris Philp: I have not heard that idea suggested. I will think about it. I do not want to respond off the cuff, but I will give consideration to the proposal. Henry VIII powers, which are essentially what the hon. Lady is describing—an ability through secondary legislation effectively to change primary legislation—are obviously viewed askance by some colleagues if too wide in scope. We do use them, of course, but normally in relatively limited circumstances. Creating a brand new criminal offence via what amounts to a Henry VIII power would be quite a wide application of the power, but it is an idea that I am perfectly happy to go away and reflect on. I thank her for mentioning the idea.

A couple of examples were given about companies that have failed in the past. Carillion was not a financial services company and there was no regulatory oversight of the company at all. In relation to financial services regulation, despite the much stricter regulation that existed in the run-up to the 2008 financial crisis, that crisis occurred none the less. *[Interruption.]* We were not in government at the time. We should be clear-eyed about the limits of what regulation alone can deliver, but that does not deter us from taking the steps we are taking here, which I think are extremely potent, for all the reasons that I mentioned and will not repeat.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 1]

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 7 stand part.

Clauses 21 and 22 stand part.

My view is that the stand part debate on clause 6 has effectively already been had, but I will not be too heavy-handed about that at the moment.

Alex Davies-Jones: On clause 7, as I have previously mentioned, we were all pleased to see the Government bring in more provisions to tackle pornographic content online, much of which is easily accessible and can cause harm to those viewing it and potentially to those involved in it.

As we have previously outlined, a statutory duty of care for social platforms online has been missing for far too long, but we made it clear on Second Reading that such a duty will only be effective if we consider the systems, business models and design choices behind how platforms operate. For too long, platforms have been abuse-enabling environments, but it does not have to be this way. The amendments that we will shortly consider are largely focused on transparency, as we all know that the duties of care will only be effective if platforms are compelled to proactively supply their assessments to Ofcom.

On clause 21, the duty of care approach is one that the Opposition support and it is fundamentally right that search services are subject to duties including illegal content risk assessments, illegal content assessments more widely, content reporting, complaints procedures, duties about freedom of expression and privacy, and duties around record keeping. Labour has long held the view that search services, while not direct hosts of potentially damaging content, should have responsibilities that see them put a duty of care towards users first, as we heard in our evidence sessions from HOPE not hate and the Antisemitism Policy Trust.

It is also welcome that the Government have committed to introducing specific measures for regulated search services that are likely to be accessed by children. However, those measures can and must go further, so we will be putting forward some important amendments as we proceed.

Labour does not oppose clause 22, either, but I would like to raise some important points with the Minister. We do not want to be in a position whereby those designing, operating and using a search engine in the United Kingdom are subject to a second-rate internet experience. We also do not want to be in a position where we are forcing search services to choose what is an appropriate design for people in the UK. It would be worrying indeed if our online experience vastly differed from that of, let us say, our friends in the European Union. How exactly will clause 22 ensure parity? I would be grateful if the Minister could confirm that before we proceed.

Chris Philp: The shadow Minister has already touched on the effect of these clauses: clause 6 sets out duties applying to user-to-user services in a proportionate and risk-based way; clause 7 sets out the scope of the various duties of care; and clauses 21 and 22 do the same in relation to search services.

In response to the point about whether the duties on search will end up providing a second-rate service in the United Kingdom, I do not think that they will. The duties have been designed to be proportionate and reasonable. Throughout the Bill, Members will see that there are separate duties for search and for user-to-user services. That is reflected in the symmetry—which appears elsewhere, too—of clauses 6 and 7, and clauses 21 and 22. We have done that because we recognise that search is different. It indexes the internet; it does not provide a user-to-user service. We have tried to structure these duties in a way that is reasonable and proportionate, and that will not adversely impair the experience of people in the UK.

I believe that we are ahead of the European Union in bringing forward this legislation and debating it in detail, but the European Union is working on its Digital Services Act. I am confident that there will be no disadvantage to people conducting searches in United Kingdom territory.

Question put and agreed to.

Clause 6 accordingly ordered to stand part of the Bill.

Clause 7 ordered to stand part of the Bill.

Clause 8

Illegal content risk assessment duties

Alex Davies-Jones: I beg to move amendment 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."

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

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

Members will note that amendments 17 and 28 form part of a separate group. I hope that is clear.

Alex Davies-Jones: At this stage, I will speak to clause 8 and our amendments 10, 14, 25, 19 and 17.

The Chair: Order. This is confusing. The hon. Lady said "and 17". Amendment 17 is part of the next group of amendments.

Alex Davies-Jones: Apologies, Sir Roger; I will speak to amendments 10, 14, 25 and 19.

The Chair: It's all right, we'll get there.

Alex Davies-Jones: The Opposition welcome the moves to ensure that all user-to-user services are compelled to provide risk assessments in relation to illegal content, but there are gaps, ranging from breadcrumbing to provisions for the production of livestreaming of otherwise illegal content.

Labour is extremely concerned by the lack of transparency around the all-important illegal content risk assessments, which is why we have tabled amendment 10. The effectiveness of the entire Bill is undermined unless the Government commit to a more transparent approach more widely. As we all know, in the Bill currently, the vital risk assessments will only be made available to the regulator, rather than for public scrutiny. There is a real risk—for want of a better word—in that approach, as companies could easily play down or undermine the risks. They could see the provision of the risk assessments to Ofcom as a simple, tick-box exercise to satisfy the requirements of them, rather than using the important assessments as an opportunity truly to assess the likelihood of current and emerging risks.

As my hon. Friend the Member for Worsley and Eccles South will touch on in her later remarks, the current approach runs the risk of allowing businesses to shield themselves from true transparency. The Minister knows that this is a major issue, and that until service providers and platforms are legally compelled to provide data, we will be shielded from the truth, because there is no statutory requirement for them to be transparent. That is fundamentally wrong and should not be allowed to continue. If the Government are serious about their commitment to transparency, and to the protection of adults and children online, they should make this small concession and see it as a positive step forward.

Amendment 14 would ensure that regulated companies, boards or senior staff have appropriate oversight of risk assessments related to adults. An obligation on boards or senior managers to approve risk assessments would hardwire the safety duties and create a culture of compliance in the regulated firms. The success of the 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.

To date, boards and top executives of the regulated companies have not taken the risks to children seriously enough. Platforms either have not considered producing risk assessments or, if they have done so, they have been of limited efficiency and have demonstrably failed to adequately identify and respond to harms to children. Need I remind the Minister that the Joint Committee on the draft Bill recommended that risk assessments should be approved at board level?

Introducing a requirement on regulated companies 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 will trickle down the organisation and help embed a culture of compliance across the company. We need to see safety online as a key focus for these platforms, and putting the onus on senior managers to take responsibility is a positive step forward in that battle.

11 am

On amendment 25, the Opposition fully support the Bill's ambition to hold regulated services accountable for online sexual exploitation of children occurring on their platforms. The implications of the duties of care introduced by the Bill will be felt around the world in the prevention, disruption and detection of online sexual exploitation of children.

We are encouraged by the prioritisation of tackling the dissemination of child sexual exploitation and abuse. However, there is room for the Bill to go even further in strengthening child protection online, particularly in relation to the use of online platforms to generate new child sexual exploitation and abuse content. While it is a welcome step forward that the Bill is essentially encouraging a safety-by-design approach, clause 8 does not go far enough to tackle newly produced content or livestreamed content.

The Minister will be aware of the huge problems with online sexual exploitation of children. I pay tribute to the hard work of my hon. Friend the Member for Rotherham (Sarah Champion), alongside the International Justice Mission, which has been a particularly vocal champion of vulnerable young children at home and abroad.

The Philippines is a source country for livestreamed sexual exploitation of children. In its recent white paper, the IJM found that traffickers often use cheap Android smartphones with prepaid cellular data services to communicate with customers to produce and distribute explicit material. In order to reach the largest possible customer base, they often connect with sexually motivated offenders through everyday technology—the same platforms that the rest of us use to communicate with friends, family and co-workers.

One key issue with assessing the extent of online sexual exploitation of children is that we are entirely dependent on detection of the crime. Sadly, most current technologies widely used to detect various forms of online sexual exploitation of children are not designed to recognise livestreaming. Clearly, the implications of that are huge for both child sexual exploitation and human trafficking more widely. The International Justice Mission reports that file hashtag and PhotoDNA, which are widely used to great effect in enabling the detection and reporting of millions of known child sexual exploitation files, do not and cannot detect newly produced child sexual exploitation material.

The livestreaming of CSEM involves an ephemeral video stream, not a stored still or a video file. It is also therefore not usually subject to screening or content review. We must consider how easy it is for platforms to host live content and how ready they are to screen that content. I need only point the Minister to the devastating mass shooting that took place in Buffalo last month. The perpetrator livestreamed the racist attack online, using a GoPro camera attached to a military-style helmet. The shooter streamed live on the site Twitch for around two minutes before the site took the livestream down, but since then the video has been posted elsewhere on the internet and on smaller platforms.

Other white supremacists have used social media to publicise gruesome attacks, including the mass shooter in Christchurch, New Zealand, in 2019. Since that shooting, social media companies have got better in some ways at combating videos of atrocities online, including stopping livestreams of attacks faster, but violent videos, such as those of mass shootings, are saved by users and then reappear across the internet on Facebook, Instagram, Twitter, TikTok and other high-harm, smaller platforms. These reuploaded videos are harder for companies to take down. Ultimately, more needs to be done at the back end in terms of design features if we are to truly make people safe.

When it comes to exploitation being livestreamed online—unlike publicised terror attacks—crimes that are not detected are not reported. Therefore, livestreaming of child sexual exploitation is a severely under-reported crime and reliable figures for its prevalence do not exist. Anecdotally, the problem in the Philippines is overwhelming, but it is not limited to the Philippines. The IJM is aware of similar child trafficking originating from other source countries in south-east Asia, south Asia, Africa and Europe. Therefore, it is essential that technology companies and online platforms are compelled to specifically consider the production of illegal content when drawing up their risk assessments.

I turn to amendment 19, which we tabled to probe the Minister on how well he believes the clause encapsulates the cross-platform risk that children may face online. Organisations such as the National Society for the Prevention of Cruelty to Children and 5Rights have raised concerns that, as the Bill is drafted, there is a gap where children are groomed on one platform, where no abuse takes place, but are then directed to another platform, where they are harmed.

Well-established grooming pathways see abusers exploit the design features of social networks to contact children before moving communication across to other platforms, including livestreaming sites and encrypted messaging services. Perpetrators manipulate features such as Facebook's algorithmic friend suggestions to make initial contact with large numbers of children whereby they can use direct messages to groom children and then coerce them into sending sexual images via WhatsApp.

Similarly, an abuser might groom a child through playing video games and simultaneously building that relationship further via a separate chat platform such as Discord. I want to point colleagues to Frida. Frida was groomed at the age of 13, and Frida's story sadly highlights the subtle ways in which abusers can groom children on social networks before migrating them to other, more harmful apps and sites.

This is Frida's experience in her own words:

> "When I was 13, a man in his 30s contacted me on Facebook. I added him because you just used to add anyone on Facebook. He started messaging me and I like the attention. We'd speak every day, usually late at night for hours at a time. We started using WhatsApp to message. He started asking for photos so I sent some. Then he asked for some explicit photos so I did that too, and he reciprocated. He told me he'd spoken to other girls online and lied about his age to them, but he didn't lie to me so I felt like I could trust him."

Frida was 13 years old. How many other Fridas are there?

We recognise that no online service can assemble every piece of the jigsaw. However, the Bill does not place requirements on services to consider how abuse spreads from their platform to others or vice versa, to risk-assess accordingly or to co-operate with other platforms proactively to address harm. Amendment 19 would

require companies to understand when discharging their risk assessment duties how abuse spreads from their platform to others or vice versa. For example, companies should understand how their platforms are situated on abuse pathways whereby the grooming and other online sexual abuse risks start on their site before migrating to other services, or whether they inherit risks from other sites.

Companies should also know whether they are dealing with abuse cross-platform risks, which happen sequentially, as tends to be the case for grooming initiated on social networks, or simultaneously, as tends to be the case on gaming services. Lastly, they should understand which functionalities and design features allowed child sexual exploitation offences to be committed and transferred across platforms.

The NSPCC research found that four UK adults in five think that social media companies should have a legal duty to work with each other to prevent online grooming from happening across multiple platforms, so that is an area in which the Minister has widespread support, both in the House and in the public realm.

This matter is not addressed explicitly. We are concerned that companies might be able to cite competition worries to avoid considering that aspect of online abuse. That is unacceptable. We are also concerned that forthcoming changes to the online environment such as the metaverse will create new risks such as more seamless moving of abuse between different platforms .

Kirsty Blackman: I want to talk about a few different things relating to the amendments. Speaking from the Opposition Front Bench, the hon. Member for Pontypridd covered in depth amendment 20, which relates to being directed to other content. Although this seems like a small amendment, it would apply in a significant number of different situations. Particular mention was made of Discord for gaming, but also of things such as moving from Facebook to Messenger—all those different directions that can happen. A huge number of those are important for those who would seek to abuse children online by trying to move from the higher-regulation services or ones with more foot traffic to areas with perhaps less moderation so as to attack children in more extreme ways.

I grew up on the internet and spent a huge amount of time speaking to people, so I am well aware that people can be anyone they want to be on the internet, and people do pretend to be lots of different people. If someone tells us their age on the internet, we cannot assume that that is in any way accurate. I am doing what I can to imprint that knowledge on my children in relation to any actions they are taking online. In terms of media literacy, which we will come on to discuss in more depth later, I hope that one of the key things that is being told to both children and adults is that it does not matter if people have pictures on their profile—they can be anybody that they want to online and could have taken those pictures from wherever.

In relation to amendment 21 on collaboration, the only reasonable concern that I have heard is about an action that was taken by Facebook in employing an outside company in the US. It employed an outside company that placed stories in local newspapers on concerns about vile things that were happening on TikTok. Those stories were invented—they were made up—specifically to harm TikTok's reputation. I am not saying for a second that collaboration is bad, but I think the argument that some companies may make that it is bad because it causes them problems and their opponents may use it against them proves the need to have a regulator. The point of having a regulator is to ensure that any information or collaboration that is required is done in a way that, should a company decide to use it with malicious intent, the regulator can come down on them. The regulator ensures that the collaboration that we need to happen in order for emergent issues to be dealt with as quickly as possible is done in a way that does not harm people. If it does harm people, the regulator is there to take action.

I want to talk about amendments 25 and 30 on the production of images and child sexual abuse content. Amendment 30 should potentially have an "or" at the end rather than an "and". However, I am very keen to support both of those amendments, and all the amendments relating to the production of child sexual abuse content. On the issues raised by the Opposition about livestreaming, for example, we heard two weeks ago about the percentage of self-generated child sexual abuse content. The fact is that 75% of that content is self-generated. That is absolutely huge.

If the Bill does not adequately cover production of the content, whether it is by children and young people who have been coerced into producing the content and using their cameras in that way, or whether it is in some other way, then the Bill fails to adequately protect our children. Purely on the basis of that 75% stat, which is so incredibly stark, it is completely reasonable that production is included. I would be happy to support the amendments in that regard; I think they are eminently sensible. Potentially, when the Bill was first written, production was not nearly so much of an issue. However, as it has moved on, it has become a huge issue and something that needs tackling. Like Opposition Members, I do not feel like the Bill covers production in as much detail as it should, in order to provide protection for children.

Dan Carden: Amendment 10 would create a duty to publish the illegal content risk assessment, and proactively supply that to Ofcom. This is new legislation that is really a trial that will set international precedent, and a lot of the more prescriptive elements—which are necessary—are perhaps the most challenging parts of the Bill. The Minister has been very thoughtful on some of the issues, so I want to ask him, when we look at the landscape of how we look to regulate companies, where does he stand on transparency and accountability? How far is he willing to go, and how far does the Bill go, on issues of transparency? It is my feeling that the more companies are forced to publish and open up, the better. As we saw with the case of the Facebook whistleblower Frances Haugen, there is a lot to uncover. I therefore take this opportunity to ask the Minister how far the Bill goes on transparency and what his thoughts are on that.

11.15 am

Chris Philp: Clause 8 sets out the risk assessment duties for illegal content, as already discussed, that apply to user-to-user services. Ofcom will issue guidance

[Chris Philp]

on how companies can undertake those. To comply with those duties, companies will need to take proportionate measures to mitigate the risks identified in those assessments. The clause lists a number of potential risk factors the providers must assess, including how likely it is that users will encounter illegal content, as defined later in the Bill,

"by means of the service".

That phrase is quite important, and I will come to it later, on discussing some of the amendments, because it does not necessarily mean just on the service itself but, in a cross-platform point, other sites where users might find themselves via the service. That phrase is important in the context of some of the reasonable queries about cross-platform risks.

Moving on, companies will also need to consider how the design and operation of their service may reduce or increase the risks identified. Under schedule 3, which we will vote on, or at least consider, later on, companies will have three months to carry out risk assessments, which must be kept up to date so that fresh risks that may arise from time to time can be accommodated. Therefore, if changes are made to the service, the risks can be considered on an ongoing basis.

Amendment 10 relates to the broader question that the hon. Member for Liverpool, Walton posed about transparency. The Bill already contains obligations to publish summary risk assessments on legal but harmful content. That refers to some of the potentially contentious or ambiguous types of content for which public risk assessments would be helpful. The companies are also required to make available those risk assessments to Ofcom on request. That raises a couple of questions, as both the hon. Member for Liverpool, Walton mentioned and some of the amendments highlighted. Should companies be required to proactively serve up their risk assessments to Ofcom, rather than wait to be asked? Also, should those risk assessments all be published—probably online?

In considering those two questions, there are a couple of things to think about. The first is Ofcom's capacity. As we have discussed, 25,000 services are in scope. If all those services proactively delivered a copy of their risk assessment, even if they are very low risk and of no concern to Ofcom or, indeed, any of us, they would be in danger of overwhelming Ofcom. The approach contemplated in the Bill is that, where Ofcom has a concern or the platform is risk assessed as being significant—to be clear, that would apply to all the big platforms—it will proactively make a request, which the platform will be duty bound to meet. If the platform does not do that, the senior manager liability and the two years in prison that we discussed earlier will apply.

Alex Davies-Jones: The Minister mentioned earlier that Ofcom would be adequately resourced and funded to cope with the regulatory duty set out in the Bill. If Ofcom is not able to receive risk assessments for all the platforms potentially within scope, even if those platforms are not deemed to be high risk, does that not call into question whether Ofcom has the resource needed to actively carry out its duties in relation to the Bill?

Chris Philp: Of course, Ofcom is able to request any of them if it wants to—if it feels that to be necessary—but receiving 25,000 risk assessments, including from tiny companies that basically pose pretty much no risk at all and hardly anyone uses, would, I think, be an unreasonable and disproportionate requirement to impose. I do not think it is a question of the resources being inadequate; it is a question of being proportionate and reasonable.

Dan Carden: The point I was trying to get the Minister to think about was the action of companies in going through the process of these assessments and then making that information publicly available to civil society groups; it is about transparency. It is what the sector needs; it is the way we will find and root out the problems, and it is a great missed opportunity in this Bill.

Chris Philp: To reassure the hon. Member on the point about doing the risk assessment, all the companies have to do the risk assessment. That obligation is there. Ofcom can request any risk assessment. I would expect, and I think Parliament would expect, it to request risk assessments either where it is concerned about risk or where the platform is particularly large and has a very high reach—I am thinking of Facebook and companies like that. But hon. Members are talking here about requiring Ofcom to receive and, one therefore assumes, to consider, because what is the point of receiving an assessment unless it considers it? Receiving it and just putting it on a shelf without looking at it would be pointless, obviously. Requiring Ofcom to receive and look at potentially 25,000 risk assessments strikes me as a disproportionate burden. We should be concentrating Ofcom's resources—and it should concentrate its activity, I submit—on those companies that pose a significant risk and those companies that have a very high reach and large numbers of users. I suggest that, if we imposed an obligation on it to receive and to consider risk assessments for tiny companies that pose no risk, that would not be the best use of its resources, and it would take away resources that could otherwise be used on those companies that do pose risk and that have larger numbers of users.

Kim Leadbeater: Just to be clear, we are saying that the only reason why we should not be encouraging the companies to do the risk assessment is that Ofcom might not be able to cope with dealing with all the risk assessments. But surely that is not a reason not to do it. The risk assessment is a fundamental part of this legislation. We have to be clear that there is no point in the companies having those risk assessments if they are not visible and transparent.

Chris Philp: All the companies have to do the risk assessment, for example for the "illegal" duties, where they are required to by the Bill. For the "illegal" duties, that is all of them; they have to do those risk assessments. The question is whether they have to send them to Ofcom—all of them—even if they are very low risk or have very low user numbers, and whether Ofcom, by implication, then has to consider them, because it would be pointless to require them to be sent if they were not then looked at. We want to ensure that Ofcom's resources

are pointed at the areas where the risks arise. Ofcom can request any of these. If Ofcom is concerned—even a bit concerned—it can request them.

Hon. Members are then making a slightly adjacent point about transparency—about whether the risk assessments should be made, essentially, publicly available. In relation to comprehensive public disclosure, there are legitimate questions about public disclosure and about getting to the heart of what is going on in these companies in the way in which Frances Haugen's whistleblower disclosures did. But we also need to be mindful of what we might call malign actors—people who are trying to circumvent the provisions of the Bill—in relation to some of the "illegal" provisions, for example. We do not want to give them so much information that they know how they can circumvent the rules. Again, there is a balance to strike between ensuring that the rules are properly enforced and having such a high level of disclosure that people seeking to circumvent the rules are able to work out how to do so.

Kirsty Blackman: If the rules are so bad that people can circumvent them, they are not good enough anyway and they need to be updated, but I have a specific question on this. The Minister says that Ofcom will be taking in the biggest risk assessments, looking at them and ensuring that they are adequate. Will he please give consideration to asking Ofcom to publish the risk assessments from the very biggest platforms? Then they will all be in one place. They will be easy for people to find and people will not have to rake about in the bottom sections of a website. And it will apply only in the case of the very biggest, most at risk platforms, which should be regularly updating their risk assessments and changing their processes on a very regular basis in order to ensure that people are kept safe.

Chris Philp: I thank the hon. Lady for her intervention and for the—

The Chair: Order. I am sorry to interrupt the Minister, but I now have to adjourn the sitting until this afternoon, when the Committee will meet again, in Room 9 and with Ms Rees in the Chair.

11.25 am

The Chair adjourned the Committee without Question put (Standing Order No. 88).

Adjourned till this day at Two o'clock.