

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

ONLINE SAFETY BILL

(Re-committed Clauses and Schedules)

Third Sitting

Thursday 15 December 2022

(Morning)

CONTENTS

CLAUSES 79 and 82 agreed to, with amendments.
SCHEDULE 11 agreed to, with amendments.
CLAUSES 87, 90, 115, 155, 169 and 183 agreed to, some with amendments.
SCHEDULE 17 agreed to, with amendments.
CLAUSES 203, 206 and 207 agreed to, some with amendments.
New clauses considered.
Bill, as amended, to be reported.
Written evidence reported to the House.

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

not later than

Monday 19 December 2022

© Parliamentary Copyright House of Commons 2022

This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.

The Committee consisted of the following Members:

Chairs: †DAME ANGELA EAGLE, SIR ROGER GALE

† Ansell, Caroline (*Eastbourne*) (Con)

† Bailey, Shaun (*West Bromwich West*) (Con)

Bhatti, Saqib (*Meriden*) (Con)

† Blackman, Kirsty (*Aberdeen North*) (SNP)

† Bonnar, Steven (*Coatbridge, Chryston and Bellshill*) (SNP)

† Bristow, Paul (*Peterborough*) (Con)

† Collins, Damian (*Folkestone and Hythe*) (Con)

† Davies-Jones, Alex (*Pontypridd*) (Lab)

† Fletcher, Nick (*Don Valley*) (Con)

Leadbeater, Kim (*Batley and Spen*) (Lab)

† Maclean, Rachel (*Redditch*) (Con)

† Nichols, Charlotte (*Warrington North*) (Lab)

Owen, Sarah (*Luton North*) (Lab)

Peacock, Stephanie (*Barnsley East*) (Lab)

Russell, Dean (*Watford*) (Con)

† Scully, Paul (*Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport*)

† Wood, Mike (*Dudley South*) (Con)

Kevin Maddison, Bethan Harding, *Committee Clerks*

† **attended the Committee**

Public Bill Committee

Thursday 15 December 2022

(Morning)

[DAME ANGELA EAGLE *in the Chair*]

Online Safety Bill

(Re-committed Clauses and Schedules: Clauses 11 to 14, 18 to 21, 30, 46, 55 and 65, Schedule 8, Clauses 79 and 82, Schedule 11, Clauses 87, 90, 115, 169 and 183, Schedule 17, Clauses 203, 206 and 207, new Clauses and new Schedules)

Clause 79

GENERAL DUTIES OF OFCOM UNDER SECTION 3 OF
THE COMMUNICATIONS ACT

11.30 am

Amendments made: 46, in clause 79, page 69, line 35, after “Chapter 1” insert “or 2A”.

Clause 79 is about OFCOM’s general duties. This amendment inserts a reference to Chapter 2A, which is the new Chapter expected to be formed by NC3 to NC6.

Amendment 47, in clause 79, page 70, line 9, after “Chapter 1” insert “or 2A”.

Clause 79 is about OFCOM’s general duties. This amendment inserts a reference to Chapter 2A, which is the new Chapter expected to be formed by NC3 to NC6.—(Paul Scully.)

Clause 79, as amended, ordered to stand part of the Bill.

Clause 82

MEANING OF THRESHOLD CONDITIONS ETC

The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Paul Scully): I beg to move amendment 48, in clause 82, page 72, line 21, at end insert—

“(ca) a regulated user-to-user service meets the conditions in section (List of emerging Category 1 services)(2) if those conditions are met in relation to the user-to-user part of the service;”.

This is a technical amendment ensuring that references to user-to-user services in the new clause inserted by NC7 relate to the user-to-user part of the service.

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

Government amendment 49.

Government new clause 7—*List of emerging Category 1 services.*

Paul Scully: These Government amendments confer a duty on Ofcom to create and publish a list of companies that are approaching the category 1 threshold to ensure that it proactively identifies emerging high-reach, high-influence companies and is ready to add them to the

category 1 register without delay. That is being done in recognition of the rapid pace of change in the tech industry, in which companies can grow quickly. The changes mean that Ofcom can designate companies as category 1 at pace. That responds to concerns that platforms could be unexpectedly popular and quickly grow in size, and that there could be delays in capturing them as category 1 platforms. Amendments 48 and 49 are consequential on new clause 7, which confers a duty on Ofcom to create and publish a list of companies that are approaching the category 1 threshold. For those reasons, I recommend that the amendments be accepted.

Alex Davies-Jones (Pontypridd) (Lab): It will come as no surprise to Members to hear that we have serious concerns about the system of categorisation and the threshold conditions for platforms and service providers, given our long-standing view that the approach taken is far too inflexible.

In previous sittings, we raised the concern that the Government have not provided enough clarity about what will happen if a service is required to shift from one category to another, and how long that will take. We remain unclear about that, about how shifting categories will work in practice, and about how long Ofcom will have to preside over such changes and decisions.

I have been following this Bill closely for just over a year, and I recognise that the online space is constantly changing and evolving. New technologies are popping up that will make this categorisation process even more difficult. The Government must know that their approach does not capture smaller, high-harm platforms, which we know—we have debated this several times—can be at the root of some of the most dangerous and harmful content out there. Will the Minister clarify whether the Government amendments will allow Ofcom to consider adding such small, high-harm platforms to category 1, given the risk of harm?

More broadly, we are pleased that the Government tabled new clause 7, which will require Ofcom to prepare and update a list of regulated user-to-user services that have 75% of the number of users of a category 1 service, and at least one functionality of a category 1 service, or one required combination of a functionality and another characteristic or factor of a category 1 service. It is absolutely vital that Ofcom, as the regulator, is sufficiently prepared, and that there is monitoring of regulated user-to-user services so that this regime is as flexible as possible and able to cope with the rapid changes in the online space. That is why the Opposition support new clause 7 and have not sought to amend it. Moreover, we also support Government amendments 48 and 49, which are technical amendments to ensure that new clause 7 references user-to-user services and assessments of those services appropriately. I want to press the Minister on how he thinks these categories will work, and on Ofcom’s role in that.

Kirsty Blackman (Aberdeen North) (SNP): I agree with everything that the hon. Lady said. New clause 7 is important. It was missing from the earlier iterations of the Bill, and it makes sense to have it here, but it raises further concerns about the number of people who are required to use a service before it is classed as category 1.

We will come later to our amendment 104 to schedule 11, which is about adding high-risk platforms to the categorisation.

I am still concerned that the numbers are a pretty blunt instrument for categorising something as category 1. The number may end up being particularly high. I think it would be very easy for the number to be wrong—for it to be too high or too low, and probably too high rather than too low.

If Twitter were to disappear, which, given the changing nature of the online world, is not outside the realms of possibility, we could see a significant number of other platforms picking up the slack. A lot of them might have fewer users, but the same level of risk as platforms such as Twitter and Facebook. I am still concerned that choosing a number is a very difficult thing to get right, and I am not totally convinced that the Government's way of going about this is right.

Paul Scully: Ofcom will assess services that are close to meeting the threshold conditions of category 1 services and will publish a publicly available list of those emerging high-risk services. A service would have to meet two conditions to be added to the emerging services list: it would need at least 75% of the number of user figures in any category 1 threshold condition, and at least one functionality of a category 1 threshold condition, or one specified combination of a functionality and a characteristic or factor of a category 1 threshold condition.

Ofcom will monitor the emergence of new services. If it becomes apparent that a service has grown sufficiently to meet the threshold of becoming a category 1 service, Ofcom will be required to add that service to the register. The new clause and the consequential amendments take into account the possibility of quick growth.

Following the removal of “legal but harmful” duties, category 1 services will be subject to new transparency, accountability and free speech duties, as well as duties relating to protection for journalists and democratic content. Requiring all companies to comply with that full range of category 1 duties would pose a disproportionate regulatory burden on smaller companies that do not exert the same influence on public discourse, and that would possibly divert those companies' resources away from tackling vital tasks.

Damian Collins (Folkestone and Hythe) (Con): Will my hon. Friend confirm that the risk assessments for illegal content—the priority illegal offences; the worst kind of content—apply to all services, whether or not they are category 1?

Paul Scully: My hon. Friend is absolutely right. All companies will still have to tackle the risk assessment, and will have to remove illegal content. We are talking about the extra bits that could take a disproportionate amount of resource from core functions that we all want to see around child protection.

Alex Davies-Jones: I would push the Minister further. He mentioned that there will not be an onus on companies to tackle the “legal but harmful” duty now that it has been stripped from the Bill, but we know that disinformation, particularly around elections in this country, is widespread on these high-harm platforms,

and they will not be in scope of category 2. We have debated that at length. We have debated the time it could take Ofcom to act and put those platforms into category 1. Given the potential risk of harm to our democracy as a result, will the Minister press Ofcom to act swiftly in that regard? We cannot put that in the Bill now, but time is of the essence.

Paul Scully: Absolutely. The Department has techniques for dealing with misinformation and disinformation as well, but we will absolutely push Ofcom to work as quickly as possible. As my right hon. and learned Friend the Member for Kenilworth and Southam (Sir Jeremy Wright), the former Secretary of State, has said, once an election is done, it is done and it cannot be undone.

Damian Collins: Could the Minister also confirm that the provisions of the National Security Bill read across to the Online Safety Bill? Where disinformation is disseminated by networks operated by hostile foreign states, particularly Russia, as has often been the case, that is still in scope. That will still require a risk assessment for all platforms, whether or not they are category 1.

Paul Scully: Indeed. We need to take a wide-ranging, holistic view of disinformation and misinformation, especially around election times. There is a suite of measures available to us, but it is still worth pushing Ofcom to make sure that it works as quickly as possible.

Amendment 48 agreed to.

Amendment made: 49, in clause 82, page 72, line 23, after “conditions” insert

“or the conditions in section (List of emerging Category 1 services)(2)”.—(*Paul Scully.*)

This is a technical amendment ensuring that references to assessments of user-to-user services in the new clause inserted by NC7 relate to the user-to-user part of the service.

Clause 82, as amended, ordered to stand part of the Bill.

Schedule 11

CATEGORIES OF REGULATED USER-TO-USER SERVICES AND REGULATED SEARCH SERVICES: REGULATIONS

Paul Scully: I beg to move amendment 76, in schedule 11, page 213, line 11, at end insert

“, and

- (c) any other characteristics of that part of the service or factors relating to that part of the service that the Secretary of State considers relevant.”

This amendment provides that regulations specifying Category 1 threshold conditions for the user-to-user part of regulated user-to-user services must also include conditions relating to any other characteristics of that part of the service or factors relating to that part of the service that the Secretary of State considers relevant.

The Chair: With this, it will be convenient to discuss Government amendments 77 to 79, 81 to 84, 86 to 91 and 93.

Paul Scully: These Government amendments seek to change the approach to category 1 designation, following the removal from the Bill of the adult safety duties and the concept of “legal but harmful” content. Through

[Paul Scully]

the proposed new duties on category 1 services, we aim to hold companies accountable to their terms of service, as we have said. I seek to remove all requirements on category 1 services relating to harmful content, so it is no longer appropriate to designate them with reference to harm. Consequently, the amendments in this group change the approach to designating category 1 services, to ensure that only the largest companies with the greatest influence over public discourse are designated as category 1 services.

Specifically, these amendments will ensure that category 1 services are so designated where they have functionalities that enable easy, quick and wide dissemination of user-generated content, and the requirement of category 1 services to meet a number of users threshold remains unchanged.

The amendments also give the Secretary of State the flexibility to consider other characteristics of services, as well as other relevant factors. Those characteristics might include a service's functionalities, the user base, the business model, governance, and other systems and processes. That gives the designation process greater flexibility to ensure that services are designated category 1 services only when they have significant influence over public discourse.

The amendments also seek to remove the use of criteria for content that is harmful to adults from category 2B, and we have made a series of consequential amendments to the designation process for categories 2A and 2B to ensure consistency.

Alex Davies-Jones: I have commented extensively on the flaws in the categorisation process in this and previous Committees, so I will not retread old ground. I accept the amendments in this grouping. They show that the Government are prepared to broaden the criteria for selecting which companies are likely to be in category 1. That is a very welcome, if not subtle, shift in the right direction.

The amendments bring the characteristics of a company's service into consideration, which will be a slight improvement on the previous focus on size and functionality, so we welcome them. The distinction is important, because size and functionality alone are obviously very vague indicators of harm, or the threat of harm.

We are pleased to see that the Government have allowed for a list to be drawn up of companies that are close to the margins of category 1, or that are emerging as category 1 companies. This is a positive step for regulatory certainty, and I hope that the Minister will elaborate on exactly how the assessment will be made.

However, I draw the Minister's attention to Labour's long-held concern about the Bill's over-reliance on powers afforded to the Secretary of State of the day. We debated this concern in a previous sitting. I press the Minister again on why these amendments, and the regulations around the threshold conditions, are ultimately only for the Secretary of State to consider, depending on characteristics or factors that only he or she, whoever they may be, deems relevant.

We appreciate that the regulations need some flexibility, but we have genuine concerns—indeed, colleagues from all parties have expressed such concerns—that the Bill

will give the Secretary of State far too much power to determine how the entire online safety regime is imposed. I ask the Minister to give the Committee an example of a situation in which it would be appropriate for the Secretary of State to make such changes without any consultation with stakeholders or the House.

It is absolutely key for all of us that transparency should lie at the heart of the Bill. Once again, we fear that the amendments are a subtle attempt by the Government to impose on what is supposed to be an independent regulatory process the whim of one person. I would appreciate assurance on that point. The Minister knows that these concerns have long been held by me and colleagues from all parties, and we are not alone in those concerns. Civil society groups are also calling for clarity on exactly how decisions will be made, and particularly on what information will be used to determine a threshold. For example, do the Government plan on quantifying a user base, and will the Minister explain how the regime would work in practice, when we know that a platform's user base can fluctuate rapidly? We have seen that already with Mastodon; the latter's users have increased incredibly as a result of Elon Musk's takeover of Twitter. I hope that the Minister can reassure me about those concerns. He will know that this is a point of contention for colleagues from across the House, and we want to get the Bill right before we progress to Report.

11.45 am

Kirsty Blackman: My understanding is that only a very small number of platforms will reach the category 1 threshold. We are talking about the platforms that everybody has heard of—Facebook, Twitter and so on—and not about the slightly smaller platforms that lots of people have heard of and use. We are probably not talking about platforms such as Twitch, which has a much smaller user base than Facebook and Twitter but has a massive reach. My concern continues to be that the number threshold does not take into account the significant risks of harm from some of those platforms.

I have a specific question about amendment 76. I agree with my Labour Front-Bench colleague, the hon. Member for Pontypridd, that it shows that the Government are willing to take into account other factors. However, I am concerned that the Secretary of State is somehow being seen as the arbiter of knowledge—the person who is best placed to make the decisions—when much more flexibility could have been given to Ofcom instead. From all the evidence I have heard and all the people I have spoken to, Ofcom seems much more expert in dealing with what is happening today than any Secretary of State could ever hope to be. There is no suggestion about how the Secretary of State will consult, get information and make decisions on how to change the threshold conditions.

It is important that other characteristics that may not relate to functionalities are included if we discover that there is an issue with them. For example, I have mentioned livestreaming on a number of occasions in Committee, and we know that livestreaming is inherently incredibly risky. The Secretary of State could designate livestreaming as a high-risk functionality, and it could be included, for example, in category 1. I do not know whether it will be, but we know that there are risks there. How will the Secretary of State get that information?

There is no agreement to set up a user advocacy board. The requirement for Ofcom to consult the Children's Commissioner will be brought in later, but organisations such as the National Society for the Prevention of Cruelty to Children, which deals with phone calls from children asking for help, are most aware of emerging threats. My concern is that the Secretary of State cannot possibly be close enough to the issue to make decisions, unless they are required to consult and listen to organisations that are at the coal face and that regularly support people. I shall go into more detail about high-harm platforms when we come to amendment 104.

Paul Scully: The amendments give the Secretary of State the flexibility to consider other characteristics of services as well as other relevant factors, which include functionalities, user base, business model, governance, and other systems and processes. They effectively introduce greater flexibility into the designation process, so that category 1 services are designated only if they have significant influence over public discourse. Although the Secretary of State will make the regulations, Ofcom will carry out the objective and evidence-based process, which will be subject to parliamentary scrutiny via statutory instruments. The Secretary of State will have due consultation with Ofcom at every stage, but to ensure flexibility and the ability to move fast, it is important that the Secretary of State has those powers.

Amendment 76 agreed to.

Kirsty Blackman: I beg to move amendment 104, in schedule 11, page 213, line 11, at end insert—

“(1A) Regulations made under sub-paragraph (1) must provide for any regulated user-to-user service which OFCOM assesses as posing a very high risk of harm to be included within Category 1, regardless of the number of users.”

This amendment allows Ofcom to impose Category 1 duties on user-to-user services which pose a very high risk of harm.

I would say this, but I think that this is the most important amendment. The key area that the Government are getting wrong is the way in which platforms, providers or services will be categorised. The threshold is based on the number of users. It is the number of users “and” one of those other things, not the number of users “or” one of those other things; even that would make a significant difference.

The Secretary of State talked about the places that have a significant influence over public discourse. It is perfectly possible to have a significant influence over public discourse with a small number of users, or with a number of users that does not number into the millions. We have seen the spread of conspiracy theories that have originated and been perpetuated on very small platforms—very small, shady places on the internet that none of us has experienced or even heard of. Those are the places that have a massive impact and effect.

We know that one person can have a significant impact on the world and on people's lives. We have heard about the physical harm that people can be incited to cause by the platforms they access, and the radicalisation and extremism they find themselves subject to. That can cause massive, damaging effects to anybody they choose to take physical action against, and to some of the most marginalised communities and groups in society. We are seeing an increase in the amount of hate crime and the number of people who believe conspiracy

theories, and not all of that is because of the spread of those things on Facebook and Twitter. It is because of the breadcrumbing and the spread that there can be on smaller platforms.

The most extreme views do not necessarily tip over into “illegal” or “incitement”; they do not actually say, “Please go out and kill everybody in this particular group.” They say, “This particular group is responsible for all of ills you feel and for every negative thing that is happening in your life”, and people are therefore driven to take extremist, terrorist action. That is a significant issue.

I want to talk about a couple of platforms. Kiwi Farms, which is no longer in existence and has been taken down, was a very small platform that dramatically damaged the lives of trans people in particular. It was a platform where people went to incite hatred and give out the addresses of folk who they knew were members of the trans community. Some of those people had to move to another continent to get away from the physical violence and attacks they faced as a result of the behaviour on that incredibly small platform, which very few people will have heard about.

Kiwi Farms has been taken down because the internet service providers decided that it was too extreme and they could not possibly host it any more. That was eventually recognised and change was made, but the influence that that small place had on lives—the difficulties and harm it caused—is untold. Some of that did tip over into illegality, but some did not.

I also want to talk about the places where there is a significant amount of pornography. I am not going to say that I have a problem with pornography online; the internet will always have pornography on it. It attracts a chunk of people to spend time online, and some of that pornography is on large mainstream sites. Searches for incest, underage girls, or black women being abused all get massive numbers of hits. There is a significant amount of pornography on these sites that is illegal, that pretends to be illegal or that acts against people with protected characteristics. Research has found that a significant proportion—significantly more than a half—of pornography on mainstream sites that involves black women also involves violence. That is completely and totally unacceptable, and has a massive negative impact on society, whereby it reinforces negativity and discrimination against groups that are already struggling with being discriminated against and that do not experience the privilege of a cis white man.

It is really grim that we are requiring a number of users to be specified, when we know the harm that caused by platforms that do not have 10 million or 20 million United Kingdom users. I do not know what the threshold will be, but I know it will be too high to include a lot of platforms that have a massive effect. The amendment is designed specifically to give Ofcom the power to designate as category 1 any service that it thinks has a very high risk of harm; I have not set the bar particularly low. Now that the Minister has increased the levels of transparency that will be required for category 1 platforms, it is even more important that we subject extremist sites and platforms—the radicalising ones, which are perpetuating discrimination—to a higher bar and require them to have the transparency that they need as a category 1 service. This is a place where the

[Kirsty Blackman]

Bill could really make a difference and change lives, and I am really concerned that it is massively failing to do so.

The reason I have said that it should be Ofcom's responsibility to designate category 1 services is on the basis that it has the experts who will be looking at all the risk assessments, dealing with companies on a day-to-day basis, and seeing the harms and transparencies that the rest of us will not be able to see. The reporting mechanisms will be public for only some of the category 1 platforms, and we will not be able to find out the level of information that Ofcom has, so it is right that it should be responsible for designating sites as having a very high risk of harm. That is why I tabled the amendment, which would make a massive difference to people who are the most discriminated against as it is and who are the most at risk of harm from extremism. I urge the Minister to think again.

Alex Davies-Jones: I rise briefly to support everything the hon. Member for Aberdeen North just said. We have long called for the Bill to take a harm-led approach; indeed, the Government initially agreed with us, as when it was in its first iteration it was called the Online Harms Bill rather than the Online Safety Bill. Addressing harm must be a central focus of the Bill, as we know extremist content is perpetuated on smaller, high-harm platforms; this is something that the Antisemitism Policy Trust and Hope not Hate have long called for with regards to the Bill.

I want to put on the record our huge support for the amendment. Should the hon. Lady be willing to push it to a vote—I recognise that we are small in number—we will absolutely support her.

Damian Collins: I want to speak briefly to the amendment. I totally understand the reasons that the hon. Member for Aberdeen North has tabled it, but in reality, the kinds of activities she describes would be captured anyway, because most would fall within the remit of the priority illegal harms that all platforms and user-to-user services have to follow. If there were occasions when they did not, being included in category 1 would mean that they would be subject to the additional transparency of terms of service, but the smaller platforms that allow extremist behaviour are likely to have extremely limited terms of service. We would be relying on the priority illegal activity to set the minimum safety standards, which Ofcom would be able to do.

It would also be an area where we would want to move at pace. Even if we wanted to bring in extra risk assessments on terms of service that barely exist, the time it would take to do that would not give a speedy resolution. It is important that in the way Ofcom exercises its duties, it does not just focus on the biggest category 1 platforms but looks at how risk assessments for illegal activity are conducted across a wide range of services in scope, and that it has the resources needed to do that.

Even within category 1, it is important that is done. We often cite TikTok, Instagram and Facebook as the biggest platforms, but I recently spoke to a teacher in a larger secondary school who said that by far the worst platform they have to deal with in terms of abuse,

bullying, intimidation, and even sharing of intimate images between children, is Snapchat. We need to ensure that those services get the full scrutiny they should have, because they are operating at the moment well below their stated terms of service, and in contravention of the priority illegal areas of harm.

12 noon

Paul Scully: As debated earlier, we are removing the adult safety duties from the Bill, which means that no company will face any duties related to legal but harmful content. In their place, the Government are introducing new transparency accountability, and free speech duties on category 1 services. They have been discussed in detail earlier this session.

It would not be proportionate to apply those new duties to smaller services, but, as we have heard from my hon. Friend the Member for Folkestone and Hythe, they will still have to comply with the illegal content and child safety duties if they are accessed by children. Those services have limited resources, and blanket applying additional duties on them would divert those resources away from complying with the illegal content and child safety duties. That would likely weaken the duties' impact on tackling criminal activity and protecting children.

The new duties are about user choice and accountability on the largest platforms—if users do not want to use smaller harmful sites, they can choose not to—but, in recognition of the rapid pace with which companies can grow, I introduced an amendment earlier to create a watchlist of companies that are approaching the category 1 threshold, which will ensure that Ofcom can monitor rapidly scaling companies, reduce any delay in designating companies as category 1 services, and apply additional obligations on them.

The hon. Member for Aberdeen North talked about ISPs acting with respect to Kiwi Farms. I talked on Tuesday about the need for a holistic approach. There is not one silver bullet. It is important to look at Government, the platforms, parenting and ISPs, because that makes up a holistic view of how the internet works. It is the multi-stakeholder framework of governing the internet in its entirety, rather than the Government trying to do absolutely everything. We have talked a lot about illegality, and I think that a lot of the areas in that case were illegal; the hon. Lady described some very distasteful things. None the less, with the introduction of the watchlist, I do not believe amendment 104 is required.

Kirsty Blackman: The hon. Member for Folkestone and Hythe made a good point. I do not disagree that Ofcom will have a significant role in policing platforms that are below the category 1 threshold. I am sure it will be very hands on, particularly with platforms that have the highest risk and are causing the most harm.

I still do not think that is enough. I do not think that the Minister's change with regard to emerging platforms should be based on user numbers. It is reasonable for us to require platforms that encourage extremism, spread conspiracy theories and have the most horrific pornography on them to meet a higher bar of transparency. I do not really care if they only have a handful of people working there. I am not fussed if they say, "Sorry, we can't do this." If they cannot keep people safe on their platform,

they should have to meet a higher transparency bar, provide more information on how they are meeting their terms of service and provide toggles—all those things. It does not matter how small these platforms are. What matters is that they have massive risks and cause massive amounts of harm. It is completely reasonable that we hold them to a higher regulatory bar. On that basis, I will push the amendment to a vote.

The Committee divided: Ayes 4, Noes 8.

Division No. 6]

AYES

Blackman, Kirsty
Bonnar, Steven

Davies-Jones, Alex
Nichols, Charlotte

NOES

Ansell, Caroline
Bailey, Shaun
Bristow, Paul
Collins, Damian

Fletcher, Nick
Maclean, Rachel
Scully, Paul
Wood, Mike

Question accordingly negatived.

Amendments made: 77, in schedule 11, page 213, line 16, after “other” insert

“characteristics of the search engine or”.

This amendment provides that regulations specifying Category 2A threshold conditions for the search engine of regulated search services must also include conditions relating to any other characteristics of the search engine that the Secretary of State considers relevant.

Amendment 78, in schedule 11, page 213, line 23, after “other” insert

“characteristics of that part of the service or”.

This amendment provides that regulations specifying Category 2B threshold conditions for the user-to-user part of regulated user-to-user services must also include conditions relating to any other characteristics of that part of the service that the Secretary of State considers relevant.

Amendment 79, in schedule 11, page 213, line 36, leave out from “on” to “disseminated” in line 37 and insert

“how easily, quickly and widely regulated user-generated content is”.

This amendment provides that in making regulations specifying Category 1 threshold conditions the Secretary of State must take into account the impact of certain matters in relation to which conditions must be specified on how easily, quickly and widely regulated user-generated content is disseminated by means of the service.

Amendment 80, in schedule 11, page 214, line 2, leave out from “illegal content” to “disseminated” in line 3 and insert

“and content that is harmful to children”.

This amendment is consequential on the removal of the adult safety duties (see Amendments 6, 7 and 41).

Amendment 81, in schedule 11, page 214, line 12, leave out “the relationship between”.

This amendment is consequential on Amendment 83 (which provides for additional matters that OFCOM must carry out research into).

Amendment 82, in schedule 11, page 214, line 13, leave out from beginning to “by” and insert

“how easily, quickly and widely regulated user-generated content is disseminated”.

This amendment provides that research required to be carried out by OFCOM before regulations specifying Category 1 threshold conditions may be made must include research into how easily, quickly and widely regulated user-generated content is disseminated by means of regulated user-to-user services.

Amendment 83, in schedule 11, page 214, line 16, at end insert

“, and

(c) such other characteristics of that part of such services or factors relating to that part of such services as OFCOM consider to be relevant to specifying the Category 1 threshold conditions.”

This amendment provides that research required to be carried out by OFCOM before regulations specifying Category 1 threshold conditions may be made must include research into other characteristics or factors of the user-to-user part of regulated user-to-user services as OFCOM consider relevant to specifying the Category 1 threshold conditions.

Amendment 84, in schedule 11, page 214, line 24, after “other” insert “characteristics or”.

This amendment provides that research required to be carried out by OFCOM before regulations specifying Category 2A threshold conditions may be made must also include research into characteristics of the search engine of regulated search services and combined services as OFCOM consider relevant to specifying the Category 2A threshold conditions.

Amendment 85, in schedule 11, page 214, line 29, leave out from “illegal content” to “by” in line 30 and insert

“and content that is harmful to children”.

This amendment is consequential on the removal of the adult safety duties (see Amendments 6, 7 and 41).

Amendment 86, in schedule 11, page 214, line 34, leave out “factors” and insert

“characteristics of that part of such services or factors relating to that part of such services”.

This amendment provides that research required to be carried out by OFCOM before regulations specifying Category 2B threshold conditions may be made must include research into such other characteristics of the user-to-user part of regulated user-to-user services as OFCOM consider relevant to specifying the Category 2B threshold conditions.

Amendment 87, in schedule 11, page 214, leave out lines 40 to 42.

This amendment and Amendments 88 to 90 (which provide that OFCOM’s advice as to what provision is appropriate for regulations under paragraph 1(1), (2) or (3) of Schedule 11 to make, may include advice that the regulations include other characteristics or factors) are consequential on Amendments 76 to 78.

Amendment 88, in schedule 11, page 214, line 44, at beginning insert “characteristic or”.

This amendment and Amendments 87, 89 and 90 (which provide that OFCOM’s advice as to what provision is appropriate for regulations under paragraph 1(1), (2) or (3) of Schedule 11 to make, may include advice that the regulations include other characteristics or factors) are consequential on Amendments 76 to 78.

Amendment 89, in schedule 11, page 214, line 45, leave out “1(3)” and insert “1(1) or (3)”.

This amendment and Amendments 87, 88 and 90 (which provide that OFCOM’s advice as to what provision is appropriate for regulations under paragraph 1(1), (2) or (3) of Schedule 11 to make, may include advice that the regulations include other characteristics or factors) are consequential on Amendments 76 to 78.

Amendment 90, in schedule 11, page 214, line 45, after “other” insert “characteristic or”.

This amendment and Amendments 87 to 89 (which provide that OFCOM’s advice as to what provision is appropriate for regulations under paragraph 1(1), (2) or (3) of Schedule 11 to make, may include advice that the regulations include other characteristics or factors) are consequential on Amendments 76 to 78.

Amendment 91, in schedule 11, page 216, line 38, at end insert—

“5A In this Schedule the ‘characteristics’ of a user-to-user part of a service or a search engine include its user base, business model, governance and other systems and processes.”

This amendment defines “characteristics” of a user-to-user part of a service or search engine for the purposes of Schedule 11.

Amendment 92, in schedule 11, page 216, leave out lines 43 and 44.

This amendment is consequential on Amendment 41 (removal of clause 55).

Amendment 93, in schedule 11, page 216, line 44, at end insert—

“‘regulated user-generated content’ has the same meaning as in Part 3 (see section 50);”—(*Paul Scully.*)

This amendment defines “regulated user-generated content” for the purposes of Schedule 11.

Schedule 11, as amended, agreed to.

Clause 87

POWER TO REQUIRE INFORMATION

Amendment made: 50, in clause 87, page 78, line 18, at end insert—

“(iiiia) any duty set out in section (Duty not to act against users except in accordance with terms of service) or (Further duties about terms of service) (terms of service);”—(*Paul Scully.*)

This amendment mentions the new duties imposed by NC3 and NC4 in the clause that sets out the purposes for which OFCOM may require people to provide information.

Clause 87, as amended, ordered to stand part of the Bill.

Clause 90

REPORTS BY SKILLED PERSONS

Amendments made: 51, in clause 90, page 82, line 5, leave out “12,”.

This amendment is consequential on Amendment 6 (removal of clause 12).

Amendment 52, in clause 90, page 82, line 8, leave out sub-paragraph (iv).

This amendment is consequential on Amendment 7 (removal of clause 13).

Amendment 53, in clause 90, page 82, line 16, at end insert—

“(xiia) section (Duty not to act against users except in accordance with terms of service) or (Further duties about terms of service) (terms of service);”—(*Paul Scully.*)

This amendment has the effect that OFCOM may require a skilled person’s report in relation to compliance with the new duties imposed by NC3 and NC4.

Clause 90, as amended, ordered to stand part of the Bill.

Clause 115

REQUIREMENTS ENFORCEABLE BY OFCOM AGAINST PROVIDERS OF REGULATED SERVICES

The Chair: We now come to Government amendments 54 and 55 to clause 115.

Alex Davies-Jones: I do not wish to test the Committee’s patience. I know we need to get the Bill over the line quickly, so I do not wish to delay it by talking over old ground that we covered in the previous Public Bill Committee on clauses that we support. We do support the Government on this clause, but I will make some

brief comments because, as we know, clause 115 is important. It lists the enforceable requirements for which failure to comply can trigger enforcement action.

The Chair: Order. I think the hon. Lady is speaking to clause 115. This is Government amendments 54 and 55 to clause 115. I will call you when we get to that place, which will be very soon, so stay alert.

Alex Davies-Jones: Apologies, Dame Angela. I got carried away.

Amendments made: 54, in clause 115, page 98, leave out lines 35 and 36.

This amendment is consequential on Amendments 6 and 7 (removal of clauses 12 and 13).

Amendment 55, in clause 115, page 99, line 19, at end insert—

“Section (Duty not to act against users except in accordance with terms of service)	Acting against users only in accordance with terms of service
---	---

Section (Further duties about terms of service)	Terms of service”
---	-------------------

—(*Paul Scully.*)

This amendment ensures that OFCOM are able to use their enforcement powers in Chapter 6 of Part 7 in relation to a breach of any of the new duties imposed by NC3 and NC4.

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

The Chair: We now come to clause 115 stand part.

Alex Davies-Jones: Thank you, Dame Angela—take 2.

Clause 115 focuses on the enforcement action that may be taken and will be triggered if a platform fails to comply. Given that the enforceable requirements may include, for example, duties to carry out and report on risk assessments and general safety duties, it is a shame that the Government have not seen the merits of going further with these provisions. I point the Minister to the previous Public Bill Committee, where Labour made some sensible suggestions for how to remedy the situation. Throughout the passage of the Bill, we have made it abundantly clear that more access to, and availability of, data and information about systems and processes would improve understanding of the online environment.

We cannot and should not rely solely on Ofcom to act as problems arise when they could be spotted earlier by experts somewhere else. We have already heard the Minister outline the immense task that Ofcom has ahead of it to monitor risk assessments and platforms, ensuring that platforms comply and taking action where there is illegal content and a risk to children. It is important that Ofcom has at its disposal all the help it needs.

It would be helpful if there were more transparency about how the enforcement provisions work in practice. We have repeatedly heard that without independent researchers accessing data on relevant harm, platforms will have no real accountability for how they tackle online harm. I hope that the Minister can clarify why, once again, the Government have not seen the merit of encouraging transparency in their approach. It would

be extremely valuable and helpful to both the online safety regime and the regulator as a whole, and it would add merit to the clause.

Paul Scully: We have talked about the fact that Ofcom will have robust enforcement powers. It can direct companies to take specific steps to come into compliance or to remedy failure to comply, as well as issue fines and apply to the courts for business disruption measures. Indeed, Ofcom can institute criminal proceedings against senior managers who are responsible for compliance with an information notice, when they have failed to take all reasonable steps to ensure the company's compliance with that notice. That criminal offence will commence two months after Royal Assent.

Ofcom will be required to produce enforcement guidelines, as it does in other areas that it regulates, explaining how it proposes to use its enforcement powers. It is important that Ofcom is open and transparent, and that companies and people using the services understand exactly how to comply. Ofcom will provide those guidelines. People will be able to see who are the users of the services. The pre-emptive work will come from the risk assessments that platforms themselves will need to produce.

We will take a phased approach to bringing the duties under the Bill into effect. Ofcom's initial focus will be on illegal content, so that the most serious harms can be addressed as soon as possible. When those codes of practice and guidelines come into effect, the hon. Member for Pontypridd will see some of the transparency and openness that she is looking for.

Question put and agreed to.

Clause 115, as amended, accordingly ordered to stand part of the Bill.

Clause 55

REVIEW

Amendment made: 56, in clause 155, page 133, line 27, after "Chapter 1" insert "or 2A".—(Paul Scully.)

Clause 155 is about a review by the Secretary of State of the regulatory framework established by this Bill. This amendment inserts a reference to Chapter 2A, which is the new Chapter expected to be formed by NC3 to NC6.

12.15 pm

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

Kirsty Blackman: I am glad that there is a review function in the Bill. I have been a member of a lot of Bill Committees and Delegated Legislation Committees that have considered legislation that has no review function and that says, "This will be looked at in the normal course of departmental reviews." We know that not all Departments always do such reviews. In fact, some Departments do under 50% of the reviews that they are supposed to do, and whether reviews take place is not checked. We therefore do not find out whether a piece of legislation has had the intended effect. I am sure some will have done, but some definitely will not.

If the Government do not internally review whether a Bill or piece of delegated legislation has had the effect it was supposed to have, they cannot say whether it has

been a success and cannot make informed decisions about future legislation, so having a review function in this Bill is really good. However, that function is insufficient as it is not enough for the Secretary of State to do the review and we will not see enough outputs from Ofcom.

The Bill has dominated the lives of a significant number of parliamentarians for the past year—longer, in some cases—because it is so important and because it has required so much scrutiny, thinking and information gathering to get to this stage. That work will not go away once the Bill is enacted. Things will not change or move at once, and parts of the legislation will not work as effectively as they could, as is the case for any legislation, whether moved by my Government or somebody else's. In every piece of legislation there will be things that do not pan out as intended, but a review by the Secretary of State and information from Ofcom about how things are working do not seem to be enough.

Committee members, including those on the Government Benches, have suggested having a committee to undertake the review or adding that function to the responsibilities of the Digital, Culture, Media and Sport Committee. We know that the DCMS Committee is busy and will be looking into a significant number of wide-ranging topics, so it would be difficult for it to keep a watching brief on the Online Safety Bill.

The previous Minister said that there will be some sort of reviewing mechanism, but I would like further commitment from the Government that the Bill will be kept under review and that the review process as set out will not be the only type of review that happens as things move and change and the internet develops. Many people talk about more widespread use of virtual reality, for example, but there could be other things that we have not even heard of yet. After the legislation is implemented, it will be years before every part of the Bill is in action and every requirement in the legislation is working. By the time we get to 2027-28—or whenever every part of the legislation is working—things could have changed again and be drastically different to today. Indeed, the legislation may not be fit for purpose when it first starts to work, so will the Minister provide more information about what the review process will look like on an ongoing basis? The Government say this is world-leading legislation, but how we will ensure that that is the case and that it makes a difference to the safety and experience of both children and adults online?

Paul Scully: I am glad that we are all in agreement on the need for a review. It is important that we have a comprehensive and timely review of the regulatory regime and how it is built into legislation. It is important that we understand that the legislation has the impact that we intend.

The legislation clearly sets out what the review must consider, how Ofcom is carrying out its role and if the legislation is effective in dealing with child protection, which as the hon. Lady rightly says is its core purpose. We have struck the balance of specifying two to five years after the regime comes into force, because it provides a degree of flexibility to future Ministers to judge when it should happen. None the less, I take the hon. Lady's point that technology is developing. That is why this is a front-footed first move in this legislation, when other countries are looking at what we are doing; because of that less prescriptive approach to technologies,

[Paul Scully]

the legislation can be flexible and adapt to emerging new technologies. Inevitably, this will not be the last word. Some of the things in the Digital Economy Act 2017, for example, are already out of date, as is some of the other legislation that was put in place in the early 2000s. We will inevitably come back to this, but I think we have the right balance at the moment in terms of the timing.

I do not think we need to bed in whom we consult, but wider consultation will none the less be necessary to ascertain the effectiveness of the legislation.

Damian Collins: I am following carefully what the Minister says, but I would say briefly that a lot of the debate we have had at all stages of the Bill has rested on how we believe Ofcom will use the powers it has been given, and we need to make sure that it does that. We need to ensure that it is effective and that it has the resources it needs. The hon. Member for Aberdeen North (Kirsty Blackman) makes an important point that it may not be enough to rely on a Select Committee of the Lords or the Commons having the time to do that in the detail we would want. We might need to consider either a post-legislative scrutiny Committee or some other mechanism to ensure that there is the necessary level of oversight.

Paul Scully: My hon. Friend is absolutely right. The report as is obviously has to be laid before Parliament and will form part of the package of parliamentary scrutiny. But, yes, we will consider how we can utilise the expertise of both Houses in post-legislative scrutiny. We will come back on that.

Question put and agreed to.

Clause 155, as amended, accordingly ordered to stand part of the Bill.

Clause 169

INDIVIDUALS PROVIDING REGULATED SERVICES:
LIABILITY

Amendment made: 57, in clause 169, page 143, line 15, at end insert—

“(fa) Chapter 2A of Part 4 (terms of service: transparency, accountability and freedom of expression);”—(*Paul Scully.*)

Clause 169 is about liability of providers who are individuals. This amendment inserts a reference to Chapter 2A, which is the new Chapter expected to be formed by NC3 to NC6, so that individuals may be jointly and severally liable for the duties imposed by that Chapter.

Clause 169, as amended, ordered to stand part of the Bill.

Clause 183 ordered to stand part of the Bill.

Schedule 17

VIDEO-SHARING PLATFORM SERVICES: TRANSITIONAL
PROVISION ETC

Amendments made: 94, in schedule 17, page 235, line 43, leave out paragraph (c).

This amendment is consequential on Amendment 6 (removal of clause 12).

Amendment 95, in schedule 17, page 236, line 27, at end insert—

“(da) the duties set out in sections (Duty not to act against users except in accordance with terms of service) and (Further duties about terms of service) (terms of service);”—(*Paul Scully.*)

This amendment ensures that services already regulated under Part 4B of the Communications Act 2003 (video-sharing platform services) are not required to comply with the new duties imposed by NC3 and NC4 during the transitional period.

Question proposed, That the schedule, as amended, be the Seventeenth schedule to the Bill.

Alex Davies-Jones: Labour welcomes schedule 17, which the Government introduced on Report. We see this schedule as clarifying exactly how the existing video-sharing platform regime will be repealed and the transitional provisions that will apply to those providers as they transition to the online safety framework. The schedule is fundamentally important for both providers and users, as it establishes the formal requirements of these platforms as we move the requirement to this new legislation.

We welcome the clarification in paragraph 1(1) of the definition of a qualifying video-sharing service. On that point, I would be grateful if the Minister clarified the situation around livestreaming video platforms and whether this schedule would also apply to them. Throughout this Bill Committee, we have heard just how dangerous and harmful live video-sharing platforms can be, so this is an important point to clarify.

I have spoken at length about the importance of capturing the harms on these platforms, particularly in the context of child sexual exploitation being livestreamed online, which, thanks to the brilliant work of International Justice Mission, we know is a significant and widespread issue. I must make reference to the IJM’s findings from its recent White Paper, which highlighted the extent of the issue in the Philippines, which is widely recognised as a source country for livestreamed sexual exploitation of children. It found that traffickers often use cheap Android smartphones with pre-paid cellular data services to communicate with customers and produce and distribute explicit material. 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 in assessing the extent of online sexual exploitation of children is that we are entirely dependent on the detection of the crime, but the reality is that most current technologies that are widely used to detect various forms of online sexual exploitation of children are not designed to recognise livestreaming video services. This is an important and prolific issue, so I hope the Minister can assure me that the provisions in the schedule will apply to those platforms too.

Paul Scully: We are setting out in schedule 17 how the existing video-sharing platform regime will be repealed in the transitional provisions that apply to these providers as they transition to the online safety framework. My understanding is that it does include livestreaming, but I will obviously write to the hon. Lady if I have got that wrong. I am not sure there is a significant legal effect here. To protect children and treat services fairly while

avoiding unnecessary burdens on business, we are maintaining the current user protections in the VSP regime while the online safety framework is being implemented. That approach to transition avoids the duplication of regulation.

Question put and agreed to.

Schedule 17, as amended, accordingly agreed to.

Clause 203

INTERPRETATION: GENERAL

Kirsty Blackman: I beg to move amendment 105, in clause 203, page 167, line 8, after “including” insert “but not limited to”.

This amendment makes clear that the definition provided for content is not exhaustive.

I am delighted that we have a new Minister, because I can make exactly the same speech as I made previously in Committee—don’t worry, I won’t—and he will not know.

I still have concerns about the definition of “content”. I appreciate that the Government have tried to include a number of things in the definition. It currently states:

“‘content’ means anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description”.

That is pretty wide-ranging, but I do not think it takes everything into account. I know that it uses the word “including”; it does not say “only limited to” or anything like that. If there is to be a list of stuff, it should be exhaustive. That is my idea of how the Bill should be.

I have suggested in amendment 105 that we add “not limited to” after “including” in order to be absolutely clear that the content that we are talking about includes anything. It may or may not be on this list. Something that is missing from the list is VR technology. If someone is using VR or immersive technology and is a character on the screen, they can see what the character is doing and move their body around as that character, and whatever they do is user-generated content. It is not explicitly included in the Bill, even though there is a list of things. I do not even know how that would be written down in any way that would make sense.

I have suggested adding “not limited to” to make it absolutely clear that this is not an exhaustive list of the things that could be considered to be user-generated content or content for the purposes of the Bill. It could be absolutely anything that is user-generated. If the Minister is able to make it absolutely clear that this is not an exhaustive list and that “content” could be anything that is user-generated, I will not press the amendment to a vote. I would be happy enough with that commitment.

Paul Scully: Indeed I can give that commitment. This is an indicative list, not an exhaustive list, for the reasons that the hon. Lady set out. Earlier, we discussed the fact that technology moves on, and she has come up with an interesting example. It is important to note that adding unnecessary words in legislation could lead to unforeseen outcomes when it is interpreted by courts, which is why we have taken this approach, but we think it does achieve the same thing.

Kirsty Blackman: On that basis, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Amendment proposed: 58, in clause 203, page 167, leave out lines 26 to 31. —(*Paul Scully.*)

This amendment removes the definition of the “maximum summary term for either-way offences”, as that term has been replaced by references to the general limit in a magistrates’ court.

12.30 pm

Kirsty Blackman: I would like to ask the Minister why this amendment has been tabled. I am not entirely clear. Could he give us some explanation of the intention behind the amendment? I am pretty sure it will be fine but, if he could just let us know what it is for, that would be helpful.

Paul Scully: I am happy to do so. Clause 203 sets out the interpretation of the terms used throughout the Bill. Amendment 58 removes a definition that is no longer required because the term is no longer in the Bill. It is as simple as that. The definition of relevant crime penalties under the Bill now uses a definition that has been updated in the light of changes to sentencing power in magistrates courts set out in the Judicial Review And Courts Act 2022. The new definition of

“general limit in a magistrates court”

is now included in the Interpretation Act 1978, so no definition is required in this Bill.

Question put and agreed to.

Amendment 58 accordingly agreed to.

Amendment made: 59, in clause 203, page 168, line 48, at end insert—

“and references to restrictions on access to a service or to content are to be read accordingly.” —(*Paul Scully.*)

NC2 states what is meant by restricting users’ access to content, and this amendment makes it clear that the propositions in clause 203 about access read across to references about restricting access.

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

Kirsty Blackman: Once again, I will abuse the privilege of having a different Minister at the Dispatch Box and mention the fact that, in the definitions, “oral communications” is mentioned in line 9 that we already mentioned in terms of the definition of “content”. It is “oral communications” in this part of the Bill but “aural communications” in an earlier part of the Bill. I am still baffled as to why there is a difference. Perhaps we should have both included in both of these sections or perhaps there should be some level of consistency throughout the Bill.

The “aural communications” section that I mentioned earlier in clause 50 is the one of the parts that I am particularly concerned about because it could create a loophole. That is a different spelling of the word. I asked this last time. I am not convinced that the answer I got gave me any more clarity than I had previously. I would be keen to understand why there is a difference, if the difference is intentional and what the difference therefore is between “oral” and “aural” communications in terms of the Bill. My understanding is that oral communications are ones that are said and aural communications are ones that are heard. But, for the purposes of the Bill, those two things are really the same, unless user-generated content in which there is

[Kirsty Blackman]

user-generated oral communication that no one can possibly hear is included. That surely does not fit into the definitions, because user-generated content is only considered if it is user-to-user—something that other people can see. Surely, oral communication would also be aural communication. In pretty much every instance that the Bill could possibly apply to, both definitions would mean the same thing. I understand the Minister may not have the answer to this at his fingertips, and I would be happy to hear from him later if that would suit him better.

Paul Scully: The clause provides legal certainty about the meaning of those terms as used in the Bill: things such as “content”, “encounter”, “taking down” and “terms of service”. That is what the clause is intended to do. It is intentional and is for the reasons the hon. Lady said. Oral means speech and speech only. Aural is speech and other sounds, which is what can be heard on voice calls. That includes music as well. One is speech. The other is the whole gamut.

Damian Collins: I am intrigued, because the hon. Member for Aberdeen North makes an interesting point. It is not one I have heard made before. Does the Minister think there is a distinction between oral and aural, where oral is live speech and aural is pre-recorded material that might be played back? Are those two are considered distinct?

Paul Scully: My knowledge is being tested, so I will write to the hon. Member for Aberdeen North and make that available to the Committee. Coming back to the point she made about oral and aural on Tuesday about another clause on the exclusions, as I said, we have a narrow exemption to ensure that traditional phone calls are not subject to regulation. But that does mean that if a service such as Fortnite, which she spoke about previously, enables adults and children to have one-to-one oral calls, companies will still need to address the surrounding functionality around how that happens, because to enable that might cause harm—for example if an adult can contact an unknown child. That is still captured within the Bill.

Kirsty Blackman: Platforms will have to address, for example, the ways in which users can communicate with people who are not on their friends list. Things like that and other ways in which communication can be set up will have to be looked at in the risk assessment. With Discord, for instance, where two people can speak to each other, Discord will have to look at the way those people got into contact with each other and the risks associated with that, rather than the conversation itself, even though the conversation might be the only bit that involves illegality.

Paul Scully: It is the functionalities around it that enable the voice conversation to happen.

Question put and agreed to.

Clause 203, as amended, accordingly ordered to stand part of the Bill.

Clause 206

EXTENT

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

Alex Davies-Jones: I would like to welcome the Government’s clarification, particularly as an MP representing a devolved nation within the UK. It is important to clarify the distinction between the jurisdictions, and I welcome that this clause does that.

Question put and agreed to.

Clause 206 accordingly ordered to stand part of the Bill.

Clause 207

COMMENCEMENT AND TRANSITIONAL PROVISION

Amendment made: 60, in clause 207, page 173, line 15, leave out “to” and insert “and”.—(Paul Scully.)

This amendment is consequential on amendment 41 (removal of clause 55).

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

Alex Davies-Jones: Labour welcomes clause 207, which outlines the commencement and transitional provisions for the Bill to effectively come into existence. The Minister knows that Labour is concerned about the delays that have repeatedly held up the Bill’s progress, and I need not convince him of the urgent need for it to pass. I think contributions in Committee plus those from colleagues across the House as the Bill has progressed speak for themselves. The Government have repeatedly claimed they are committed to keeping children safe online, but have repeatedly failed to bring forward this legislation. We must now see commitments from the Minister that the Bill, once enacted, will make a difference right away.

Labour has specific concerns shared with stakeholders, from the Age Verification Providers Association to the Internet Watch Foundation, the NSPCC and many more, about the road map going forward. Ofcom’s plan for enforcement already states that it will not begin enforcement on harm to children from user-to-user content under part 3 of the Bill before 2025. Delays to the Bill as well as Ofcom’s somewhat delayed enforcement plans mean that we are concerned that little will change in the immediate future or even in the short term. I know the Minister will stand up and say that if the platforms want to do the right thing, there is nothing stopping them from doing so immediately, but as we have seen, they need convincing to take action when it counts, so I am not convinced that platforms will do the right thing.

Charlotte Nichols (Warrington North) (Lab): If the Government’s argument is that there is nothing to stop platforms taking such actions early, why are we discussing the Bill at all? Platforms have had many years to implement such changes, and the very reason we need this Bill is that they have not been.

Alex Davies-Jones: Exactly. My hon. Friend makes an incredibly important point that goes to the heart of why we are here in the first place. If the platforms were not motivated by commercial interest and we could trust them to do the right thing on keeping children safe

and reducing harm on their platforms, we would not require this legislation in the first place. But sadly, we are where we are, which is why it is even more imperative that we get on with the job, that Ofcom is given the tools to act swiftly and tries to reduce the limit of when they come into effect and that this legislation is enacted so that it actually makes a lasting difference.

Ofcom has already been responsible for regulating video-sharing platforms for two years, yet still, despite being in year 3, it is only asking websites to provide a plan as to how they will be compliant. That means the reality is that we can expect little on child protection before 2027-28, which creates a massive gap compared with public expectations of when the Bill will be passed. We raised these concerns last time, and I felt little assurance from the Minister in post last time, so I am wondering whether the current Minister can improve on his predecessor by ensuring a short timeline for when exactly the Bill can be implemented and Ofcom can act.

We all understand the need for the Bill, which my hon. Friend the Member for Warrington North just pointed out. That is why we have been supportive in Committee and throughout the passage of the Bill. But the measures that the Bill introduces must come into force as soon as is reasonably possible. Put simply, the industry is ready and users want to be protected online and are ready too. It is just the Government, sadly, and the regulator that would be potentially holding up implementation of the legislation.

The Minister has failed to concede on any of the issues that we have raised in Committee, despite being sympathetic and supportive. His predecessor was also incredibly supportive and sympathetic on everything we raised in Committee, yet failed to take into account a single amendment or issue that we raised. I therefore make a plea to this Minister to at least see the need to press matters and the timescale that is needed here. We have not sought to formally amend this clause, so I seek the Minister's assurance that this legislation will be dealt with swiftly. I urge him to work with Labour, SNP colleagues and colleagues across the House to ensure that the legislation and the provisions in it are enacted and that there are no further unnecessary delays.

Paul Scully: Our intention is absolutely to get this regime operational as soon as possible after Royal Assent. We have to get to Royal Assent first, so I am looking forward to working with all parties in the other House to get the legislation to that point. After that, we have to ensure that the necessary preparations are completed effectively and that service providers understand exactly what is expected of them. To answer the point made by the hon. Member for Warrington North about service providers, the key difference from what happened in the years that led to this legislation being necessary is that they now will know exactly what is expected of them—and it is literally being expected of them, with legislation and with penalties coming down the line. They should not be needing to wait for the day one switch-on. They can be testing and working through things to ensure that the system does work on day one, but they can do that months earlier.

The legislation does require some activity that can be carried out only after Royal Assent, such as public consultation or laying of secondary legislation. The secondary legislation is important. We could have put

more stuff in primary legislation, but that would belie the fact that we are trying to make this as flexible as possible, for the reasons that we have talked about. It is so that we do not have to keep coming back time and again for fear of this being out of date almost before we get to implementation in the first place.

However, we are doing things at the moment. Since November 2020, Ofcom has begun regulation of harmful content online through the video-sharing platform regulatory regime. In December 2020, Government published interim codes of practice on terrorist content and activity and sexual exploitation and abuse online. Those will help to bridge the gap until the regulator becomes operational. In June 2021, we published “safety by design” guidance, and information on a one-stop-shop for companies on protecting children online. In July 2021, we published the first Government online media literacy strategy. We do encourage stakeholders, users and families to engage with and help to promote that wealth of material to minimise online harms and the threat of misinformation and disinformation. But clearly, we all want this measure to be on the statute book and implemented as soon as possible. We have talked a lot about child protection, and that is the core of what we are trying to do here.

Question put and agreed to.

Clause 207, as amended, accordingly ordered to stand part of the Bill.

New Clause 1

OFCOM'S GUIDANCE: CONTENT THAT IS HARMFUL TO CHILDREN AND USER EMPOWERMENT

“(1) OFCOM must produce guidance for providers of Part 3 services which contains examples of content or kinds of content that OFCOM consider to be, or consider not to be— OFCOM must produce guidance for providers of Category 1 services which contains examples of content or kinds of content that OFCOM consider to be, or consider not to be, content to which section 14(2) applies (see section 14(8A)).

- (a) primary priority content that is harmful to children, or
- (b) priority content that is harmful to children.

(2) Before producing any guidance under this section (including revised or replacement guidance), OFCOM must consult such persons as they consider appropriate.

(3) OFCOM must publish guidance under this section (and any revised or replacement guidance).”—(*Paul Scully.*)

This new clause requires OFCOM to give guidance to providers in relation to the kinds of content that OFCOM consider to be content that is harmful to children and content relevant to the duty in clause 14(2) (user empowerment).

Brought up, and read the First time.

12.45 pm

Paul Scully: I beg to move, That the clause be read a Second time.

The Government are committed to empowering adults to have greater control over their online experience, and to protecting children from seeing harmful content online. New clause 1 places a new duty on Ofcom to produce and publish guidance for providers of user-to-user regulated services, in relation to the crucial aims of empowering adults and providers having effective systems and processes in place. The guidance will provide further clarity, including through

[Paul Scully]

“examples of content or kinds of content that OFCOM consider to be...primary priority”

or

“priority content that is harmful to children.”

Ofcom will also have to produce guidance that sets out examples of content that it considers to be relevant to the user empowerment duties, as set out in amendment 15 to clause 14.

It is really important that expert opinion is considered in the development of this guidance, and the new clause places a duty on Ofcom to consult with relevant persons when producing sets of guidance. That will ensure that the views of subject matter experts are reflected appropriately.

Alex Davies-Jones: Labour is pleased to see the introduction of the new clause, which clarifies the role of Ofcom in delivering guidance to providers about their duties. Specifically, the new clause will require Ofcom to give guidance to providers on the kind of content that Ofcom considers to be harmful to children, or relevant to the user empowerment duty in clause 14. That is a very welcome addition indeed.

Labour remains concerned about exactly how these so-called user empowerment tools will work in practice—we have discussed that at length—and let us face it: we have had little assurance from the Minister on that point. We welcome the new clause, as it clarifies what guidance providers can expect to receive from Ofcom once the Bill is finally enacted. We can all recognise that Ofcom has a colossal task ahead of it—the Minister said so himself—so it is particularly welcome that the guidance will be subject to consultation with those that it deems appropriate. I can hope only that that will include the experts, and the many groups that provided expertise, support and guidance on internet regulation long before the Bill even received its First Reading, a long time ago. There are far too many of those experts and groups to list, but it is fundamental that the experts who often spot online harms before they properly emerge be consulted and included in this process if we are to truly capture the priority harms to children, as the new clause intends.

We also welcome the clarification in subsection (2) that Ofcom will be required to provide “examples of content” that would be considered to be—or not be—harmful. These examples will be key to ensuring that the platforms have nowhere to hide when it comes to deciding what is harmful; there will be no grey area. Ofcom will have the power to show them exact examples of what could be deemed harmful.

We recognise, however, that there is subjectivity to the work that Ofcom will have to do once the Bill passes. On priority content, it is most important that providers are clear about what is and is not acceptable; that is why we welcome the new clause, but we do of course wish that the Government applied the same logic to harm pertaining to adults online.

Kirsty Blackman: I am also happy to support new clause 1, but I have a couple of questions. It mentions that “replacement guidance” may be provided, which is important because, as we have said a number of times, things will change, and we will end up with a different

online experience; that can happen quickly. I am glad that Ofcom has the ability to refresh and update the guidance.

My question is about timelines. There do not seem to be any timelines in the new clause for when the guidance is required to be published. It is key that the guidance be published before companies and organisations have to comply with it. My preference would be for it to be published as early as possible. There may well need to be more work, and updated versions of the guidance may therefore need to be published, but I would rather companies had an idea of the direction of travel, and what they must comply with, as soon as possible, knowing that it might be tweaked. That would be better than waiting until the guidance was absolutely perfect and definitely the final version, but releasing it just before people had to start complying with it. I would like an assurance that Ofcom will make publishing the guidance a priority, so that there is enough time to ensure compliance. We want the Bill to work; it will not work if people do not know what they have to comply with. Assurance on that would be helpful.

Paul Scully: I absolutely give that assurance to the hon. Lady; that is important. We all want the measures to be implemented, and the guidance to be out there, as soon as possible. Just now I talked about the platforms bringing in measures as soon as possible, without waiting for the implementation period. They can do that far better if they have the guidance. We are already working with Ofcom to ensure that the implementation period is as short as possible, and we will continue to do so.

Question put and agreed to.

New clause 1 accordingly read a Second time, and added to the Bill.

New Clause 2

RESTRICTING USERS' ACCESS TO CONTENT

“(1) This section applies for the purposes of this Part.

(2) References to restricting users' access to content, and related references, include any case where a provider takes or uses a measure which has the effect that—

- (a) a user is unable to access content without taking a prior step (whether or not taking that step might result in access being denied), or
 - (b) content is temporarily hidden from a user.
- (3) But such references do not include any case where—
- (a) the effect mentioned in subsection (2) results from the use or application by a user of features, functionalities or settings which a provider includes in a service in compliance with the duty set out in section 14(2) (user empowerment), or
 - (b) access to content is controlled by another user, rather than the provider.
- (4) See also section 203(5).”—(Paul Scully.)

This new clause deals with the meaning of references to restricting users' access to content, in particular by excluding restrictions resulting from the use of user empowerment tools as described in clause 14.

Brought up, read the First and Second time, and added to the Bill.

New Clause 3

DUTY NOT TO ACT AGAINST USERS EXCEPT IN ACCORDANCE WITH TERMS OF SERVICE

“(1) A provider of a Category 1 service must operate the service using proportionate systems and processes designed to ensure that the provider does not—

- (a) take down regulated user-generated content from the service,
- (b) restrict users’ access to regulated user-generated content, or
- (c) suspend or ban users from using the service,

except in accordance with the terms of service.

(2) Nothing in subsection (1) is to be read as preventing a provider from taking down content from a service or restricting users’ access to it, or suspending or banning a user, if such an action is taken—

- (a) to comply with the duties set out in—
 - (i) section 9(2) or (3) (protecting individuals from illegal content), or
 - (ii) section 11(2) or (3) (protecting children from content that is harmful to children), or
- (b) to avoid criminal or civil liability on the part of the provider that might reasonably be expected to arise if such an action were not taken.

(3) In addition, nothing in subsection (1) is to be read as preventing a provider from—

- (a) taking down content from a service or restricting users’ access to it on the basis that a user has committed an offence in generating, uploading or sharing it on the service, or
- (b) suspending or banning a user on the basis that—
 - (i) the user has committed an offence in generating, uploading or sharing content on the service, or
 - (ii) the user is responsible for, or has facilitated, the presence or attempted placement of a fraudulent advertisement on the service.

(4) The duty set out in subsection (1) does not apply in relation to—

- (a) consumer content (see section (Interpretation of this Chapter));
- (b) terms of service which deal with the treatment of consumer content.

(5) If a person is the provider of more than one Category 1 service, the duty set out in subsection (1) applies in relation to each such service.

(6) The duty set out in subsection (1) extends only to the design, operation and use of a service in the United Kingdom, and references in this section to users are to United Kingdom users of a service.

(7) In this section—

- ‘criminal or civil liability’ includes such a liability under the law of a country outside the United Kingdom;
- ‘fraudulent advertisement’ has the meaning given by section 35;
- ‘offence’ includes an offence under the law of a country outside the United Kingdom.

(8) See also section 16 (duties to protect news publisher content).”—(*Paul Scully.*)

This new clause imposes a duty on providers of Category 1 services to ensure that they do not take down content or restrict users’ access to it, or suspend or ban users, except in accordance with the terms of service.

Brought up, read the First and Second time, and added to the Bill.

New Clause 4

FURTHER DUTIES ABOUT TERMS OF SERVICE

All services

“(1) A provider of a regulated user-to-user service must include clear and accessible provisions in the terms of service informing users about their right to bring a claim for breach of contract if—

- (a) regulated user-generated content which they generate, upload or share is taken down, or access to it is restricted, in breach of the terms of service, or
- (b) they are suspended or banned from using the service in breach of the terms of service.

Category 1 services

(2) The duties set out in subsections (3) to (7) apply in relation to a Category 1 service, and references in subsections (3) to (9) to ‘provider’ and ‘service’ are to be read accordingly.

(3) A provider must operate a service using proportionate systems and processes designed to ensure that—

- (a) if the terms of service state that the provider will take down a particular kind of regulated user-generated content from the service, the provider does take down such content;
- (b) if the terms of service state that the provider will restrict users’ access to a particular kind of regulated user-generated content in a specified way, the provider does restrict users’ access to such content in that way;
- (c) if the terms of service state cases in which the provider will suspend or ban a user from using the service, the provider does suspend or ban the user in those cases.

(4) A provider must ensure that—

- (a) terms of service which make provision about the provider taking down regulated user-generated content from the service or restricting users’ access to such content, or suspending or banning a user from using the service, are—
 - (i) clear and accessible, and
 - (ii) written in sufficient detail to enable users to be reasonably certain whether the provider would be justified in taking the specified action in a particular case, and
- (b) those terms of service are applied consistently.

(5) A provider must operate a service using systems and processes that allow users and affected persons to easily report—

- (a) content which they consider to be relevant content (see section (Interpretation of this Chapter));
- (b) a user who they consider should be suspended or banned from using the service in accordance with the terms of service.

(6) A provider must operate a complaints procedure in relation to a service that—

- (a) allows for complaints of a kind mentioned in subsection (8) to be made,
- (b) provides for appropriate action to be taken by the provider of the service in response to complaints of those kinds, and
- (c) is easy to access, easy to use (including by children) and transparent.

(7) A provider must include in the terms of service provisions which are easily accessible (including to children) specifying the policies and processes that govern the handling and resolution of complaints of a kind mentioned in subsection (8).

(8) The kinds of complaints referred to in subsections (6) and (7) are—

- (a) complaints by users and affected persons about content present on a service which they consider to be relevant content;

- (b) complaints by users and affected persons if they consider that the provider is not complying with a duty set out in any of subsections (1) or (3) to (5);
- (c) complaints by a user who has generated, uploaded or shared content on a service if that content is taken down, or access to it is restricted, on the basis that it is relevant content;
- (d) complaints by users who have been suspended or banned from using a service.

(9) The duties set out in subsections (3) and (4) do not apply in relation to terms of service which—

- (a) make provision of the kind mentioned in section 9(5) (protecting individuals from illegal content) or 11(5) (protecting children from content that is harmful to children), or
- (b) deal with the treatment of consumer content.

Further provision

(10) If a person is the provider of more than one regulated user-to-user service or Category 1 service, the duties set out in this section apply in relation to each such service.

(11) The duties set out in this section extend only to the design, operation and use of a service in the United Kingdom, and references to users are to United Kingdom users of a service.

(12) See also section 16 (duties to protect news publisher content).”—(*Paul Scully.*)

Subsections (3) to (8) of this new clause impose new duties on providers of Category 1 services in relation to terms of service that allow a provider to take down content or restrict users' access to it, or to suspend or ban users. Such terms of service must be clear and applied consistently. Subsection (1) of the clause contains a duty which, in part, was previously in clause 20 of the Bill.

Brought up, read the First and Second time, and added to the Bill.

New Clause 5

OFCOM'S GUIDANCE ABOUT DUTIES SET OUT IN SECTIONS (DUTY NOT TO ACT AGAINST USERS EXCEPT IN ACCORDANCE WITH TERMS OF SERVICE) AND (FURTHER DUTIES ABOUT TERMS OF SERVICE)

“(1) OFCOM must produce guidance for providers of Category 1 services to assist them in complying with their duties set out in sections (Duty not to act against users except in accordance with terms of service) and (Further duties about terms of service)(3) to (7).

(2) OFCOM must publish the guidance (and any revised or replacement guidance).”—(*Paul Scully.*)

This new clause requires OFCOM to give guidance to providers about complying with the duties imposed by NC3 and NC4.

Brought up, read the First and Second time, and added to the Bill.

New Clause 6

INTERPRETATION OF THIS CHAPTER

“(1) This section applies for the purposes of this Chapter.

(2) “Regulated user-generated content” has the same meaning as in Part 3 (see section 50), and references to such content are to content that is regulated user-generated content in relation to the service in question.

(3) “Consumer content” means—

- (a) regulated user-generated content that constitutes, or is directly connected with content that constitutes, an offer to sell goods or to supply services,
- (b) regulated user-generated content that amounts to an offence under the Consumer Protection from Unfair Trading Regulations 2008 (S.I. 2008/1277) (construed

in accordance with section 53: see subsections (3), (11) and (12) of that section), or

(c) any other regulated user-generated content in relation to which an enforcement authority has functions under those Regulations (see regulation 19 of those Regulations).

(4) References to restricting users' access to content, and related references, are to be construed in accordance with sections (Restricting users' access to content) and 203(5).

(5) Content of a particular kind is “relevant content” if—

- (a) a term of service, other than a term of service mentioned in section (Further duties about terms of service)(9), states that a provider may or will take down content of that kind from the service or restrict users' access to content of that kind, and
- (b) it is regulated user-generated content.

References to relevant content are to content that is relevant content in relation to the service in question.

(6) “Affected person” means a person, other than a user of the service in question, who is in the United Kingdom and who is—

- (a) the subject of the content,
- (b) a member of a class or group of people with a certain characteristic targeted by the content,
- (c) a parent of, or other adult with responsibility for, a child who is a user of the service or is the subject of the content, or
- (d) an adult providing assistance in using the service to another adult who requires such assistance, where that other adult is a user of the service or is the subject of the content.

(7) In determining what is proportionate for the purposes of sections (Duty not to act against users except in accordance with terms of service) and (Further duties about terms of service), the size and capacity of the provider of a service is, in particular, relevant.

(8) For the meaning of “Category 1 service”, see section 83 (register of categories of services).”—(*Paul Scully.*)

This new clause gives the meaning of terms used in NC3 and NC4.

Brought up, read the First and Second time, and added to the Bill.

New Clause 7

LIST OF EMERGING CATEGORY 1 SERVICES

“(1) As soon as reasonably practicable after the first regulations under paragraph 1(1) of Schedule 11 come into force (regulations specifying Category 1 threshold conditions), OFCOM must comply with subsections (2) and (3).

(2) OFCOM must assess each regulated user-to-user service which they consider is likely to meet each of the following conditions, to determine whether the service does, or does not, meet them—

- (a) the first condition is that the number of United Kingdom users of the user-to-user part of the service is at least 75% of the figure specified in any of the Category 1 threshold conditions relating to number of users (calculating the number of users in accordance with the threshold condition in question);
- (b) the second condition is that—
 - (i) at least one of the Category 1 threshold conditions relating to functionalities of the user-to-user part of the service is met, or
 - (ii) if the regulations under paragraph 1(1) of Schedule 11 specify that a Category 1 threshold condition relating to a functionality of the user-to-user part of the service must be met in combination with a Category 1 threshold condition relating to another characteristic of that part of the service

or a factor relating to that part of the service (see paragraph 1(4) of Schedule 11), at least one of those combinations of conditions is met.

(3) OFCOM must prepare a list of regulated user-to-user services which meet the conditions in subsection (2).

(4) The list must contain the following details about a service included in it—

- (a) the name of the service,
- (b) a description of the service,
- (c) the name of the provider of the service, and
- (d) a description of the Category 1 threshold conditions by reference to which the conditions in subsection (2) are met.

(5) OFCOM must take appropriate steps to keep the list up to date, including by carrying out further assessments of regulated user-to-user services.

(6) OFCOM must publish the list when it is first prepared and each time it is revised.

(7) When assessing whether a service does, or does not, meet the conditions in subsection (2), OFCOM must take such steps as are reasonably practicable to obtain or generate information or evidence for the purposes of the assessment.

(8) An assessment for the purposes of this section may be included in an assessment under section 83 or 84 (as the case may be) or carried out separately.”—(*Paul Scully.*)

This new clause requires OFCOM to prepare and keep up to date a list of regulated user-to-user services that have 75% of the number of users of a Category 1 service, and at least one functionality of a Category 1 service or one required combination of a functionality and another characteristic or factor of a Category 1 service.

Brought up, read the First and Second time, and added to the Bill.

New Clause 8

CHILD USER EMPOWERMENT DUTIES

“(1) This section sets out the duties to empower child users which apply in relation to Category 1 services.

(2) A duty to include in a service, to the extent that it is proportionate to do so, features which child users may use or apply if they wish to increase their control over harmful content.

(3) The features referred to in subsection (2) are those which, if used or applied by a user, result in the use by the service of systems or processes designed to—

- (a) reduce the likelihood of the user encountering priority content that is harmful, or particular kinds of such content, by means of the service, or
- (b) alert the user to the harmful nature of priority content that is harmful that the user may encounter by means of the service.

(4) A duty to ensure that all features included in a service in compliance with the duty set out in subsection (2) are made available to all child users.

(5) A duty to include clear and accessible provisions in the terms of service specifying which features are offered in compliance with the duty set out in subsection (2), and how users may take advantage of them.

(6) A duty to include in a service features which child users may use or apply if they wish to filter out non-verified users.

(7) The features referred to in subsection (6) are those which, if used or applied by a user, result in the use by the service of systems or processes designed to—

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

(8) A duty to include in a service features which child users may use or apply if they wish to only encounter content by users they have approved.

(9) A duty to include in a service features which child users may use or apply if they wish to filter out private messages from—

- (a) non-verified users, or
- (b) adult users, or
- (c) any user other than those on a list approved by the child user.

(10) In determining what is proportionate for the purposes of subsection (2), the following factors, in particular, are relevant—

- (a) all the findings of the most recent child risk assessment (including as to levels of risk and as to nature, and severity, of potential harm), and
- (b) the size and capacity of the provider of a service.

(11) In this section “non-verified user” means a user who has not verified their identity to the provider of a service (see section 58(1)).

(12) In this section references to features include references to functionalities and settings.”—(*Kirsty Blackman.*)

Brought up, and read the First time.

Kirsty Blackman: I beg to move, That the clause be read a Second time.

That was some stretch of procedure, Dame Angela, but we got there in the end. This new clause is about child user empowerment duties. I am really pleased that the Government have user empowerment duties in the Bill—they are a good thing—but I am confused as to why they apply only to adult users, and why children do not deserve the same empowerment rights over what they access online.

In writing the new clause, I pretty much copied clause 14, before there were any amendments to it, and added a couple of extra bits: subsections (8) and (9). In subsection (8), I have included:

“A duty to include in a service features which child users may use or apply if they wish to only encounter content by users they have approved.”

That would go a step further than the verification process and allow users to approve only people who are in their class at school, people with whom they are friends, or even certain people in their class at school, and to not have others on that list. I know that young people playing Fortnite—I have mentioned Fortnite a lot because people play it a lot—or Roblox are contacted by users whom they do not know, and there is no ability for young people to switch off some of the features while still being able to contact their friends. Users can either have no contact from anyone, or they can have a free-for-all. That is not the case for all platforms, but a chunk of them do not let users speak only to people on their friends list, or receive messages only from people on the list.

My proposed subsection (8) would ensure that children could have a “white list” of people who they believe are acceptable, and who they want to be contacted by, and could leave others off the list. That would help tackle not just online child exploitation, but the significant online bullying that teachers and children report. Children have spoken of the harms they experience as a result of people bullying them and causing trouble online; the perpetrators are mainly other children. Children would be able to remove such people from the list and so would not receive any content, messages or comments from those who make their lives more negative.

[Kirsty Blackman]

Subsection (9) is related to subsection (8); it would require a service to include

“features which child users may use or apply if they wish to filter out private messages from—

(a) non-verified users, or

(b) adult users, or

(c) any user other than those on a list approved by the child user.”

Adults looking to exploit children will use private messaging on platforms such as Instagram. Instagram has to know how old its users are, so anybody who is signed up to it will have had to provide it with their date of birth. It is completely reasonable for a child to say, “I want to filter out everything from an adult.” When we talk about children online, we are talking about anybody from zero to 18, which is a very wide age range. Some of those people will be working and paying bills, but will not have access to the empowerment features that adults have access to, because they have not yet reached that magical threshold. Some services may decide to give children access to user empowerment tools, but there is no requirement to. The only requirement in the Bill on user empowerment tools is for adults. That is not fair.

Children should have more control over the online environment. We know how many children feel sad as a result of their interactions online, and how many encounter content online that they wish they had never seen and cannot unsee. We should give them more power over that, and more power to say, “No, I don’t want to see that. I don’t want people I don’t know contacting me. I don’t want to get unsolicited messaged. I don’t want somebody messaging me, pretending that they are my friend or that they go to another school, when they are in fact an adult, and I won’t realise until it is far too late.”

The Bill applies to people of all ages. All of us make pretty crappy decisions sometimes. That includes teenagers, but they also make great decisions. If there was a requirement for them to have these tools, they could choose to make their online experience better. I do not think this was an intentional oversight, or that the Government set out to disadvantage children when they wrote the adult user empowerment clauses. I think they thought that it would be really good to have those clauses in the Bill, in order to give users a measure of autonomy over their time and interactions online. However, they have failed to include the same thing for children. It is a gap.

I appreciate that there are child safety duties, and that there is a much higher bar for platforms that have child users, but children are allowed a level of autonomy; look at the UN convention on the rights of the child. We give children choices and flexibilities; we do not force them to do every single thing they do, all day every day. We recognise that children should be empowered to make decisions where they can.

I know the Government will not accept the provision—I am not an idiot. I have never moved a new clause in Committee that has been accepted, and I am pretty sure that it will not happen today. However, if the Government were to say that they would consider, or even look at the possibility of, adding child user empowerment duties to the Bill, the internet would be a more pleasant place for

children. They are going to use it anyway; let us try to improve their online experience even more than the Bill does already.

Alex Davies-Jones: The hon. Member for Aberdeen North has outlined the case for the new clause eloquently and powerfully. She may not press it to a Division, if the Minister can give her assurances, but if she did, she would have the wholehearted support of the Opposition.

We see new clause 8 as complementing the child safety duties in the legislation. We fully welcome provisions that provide children with greater power and autonomy in choosing to avoid exposure to certain types of content. We have concerns about how the provisions would work in practice, but that issue has more to do with the Government’s triple-shield protections than the new clause.

The Opposition support new clause 8 because it aims to provide further protections, in addition to the child safety duties, to fully protect children from harmful content and to empower them. It would empower and enable them to filter out private messages from adults or non-verified users. We also welcome the measures in the new clause that require platforms and service providers to design accessible terms of service. That is absolutely vital to best protect children online, which is why we are all here, and what the legislation was designed for.

Paul Scully: The aim of the user empowerment duty is to give adults more control over certain categories of legal content that some users will welcome greater choice over. Those duties also give adult users greater control over who they interact with online, but these provisions are not appropriate for children. As the hon. Member for Aberdeen North acknowledged, there are already separate duties on services likely to be accessed by children, in scope of part 3, to undertake comprehensive risk assessments and to comply with safety duties to protect children from harm. That includes requirements to assess how many specific functionalities may facilitate the spread of harmful content, as outlined in clause 10(6)(e), and to protect children from harmful content, including content that has been designated as priority harmful content, by putting in place age-appropriate protections.

As such, children will not need to be provided with tools to control any harmful content they see, as the platform will need to put in place age-appropriate protections. We do not want to give children an option to choose to see content that is harmful to them. The Bill also outlines in clause 11(4)(f) that, where it is proportionate to do so, service providers will be required to take measures in certain areas to meet the child-safety duties. That includes functionalities allowing for control over content that is encountered. It would not be appropriate to require providers to offer children the option to verify their identity, due to the safeguarding and data protection risks that that would pose. Although we expect companies to use technologies such as age assurance to protect children on their service, they would only be used to establish age, not identity.

The new clause would create provisions to enable children to filter out private messages from adults and users who are not on an approved list, but the Bill already contains provisions that address the risks of adults contacting children. There are also requirements

on service providers to consider how their service could be used for grooming or child sexual exploitation and abuse, and to apply proportionate measures to mitigate those risks. The service providers already have to assess and mitigate the risks. They have to provide the risk assessment, and within it they could choose to mitigate risk by requiring services to prevent unknown users from contacting children.

For the reasons I have set out, the Bill already provides strong protections for children on services that they are likely to access. I am therefore not able to accept the new clause, and I hope that the hon. Member for Aberdeen North will withdraw it.

Kirsty Blackman: That was one of the more disappointing responses from the Minister, I am afraid. I would appreciate it if he could write to me to explain which part of the Bill provides protection to children from private messaging. I would be interested to have another look at that, so it would be helpful if he could provide details.

We do not want children to choose to see unsafe stuff, but the Bill is not strong enough on stuff like private messaging or the ability of unsolicited users to contact children, because it relies on the providers noticing that in their risk assessment, and putting in place mitigations after recognising the problem. It relies on the providers being willing to act to keep children safe in a way that they have not yet done.

When I am assisting my children online, and making rules about how they behave online, the thing I worry most about is unsolicited contact: what people might say to them online, and what they might hear from adults online. I am happy enough for them to talk to their friends online—I think that is grand—but I worry about what adults will say to them online, whether by private messaging through text or voice messages, or when they are playing a game online with the ability for a group of people working as a team together to broadcast their voices to the others and say whatever they want to say.

Lastly, one issue we have seen on Roblox, which is marketed as a children's platform, is people creating games within it—people creating sex dungeons within a child's game, or having conversations with children and asking the child to have their character take off their clothes. Those things have happened on that platform, and I am concerned that there is not enough protection in place, particularly to address that unsolicited contact. Given the disappointing response from the Minister, I am keen to push this clause to a vote.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 8.

Division No. 7]

AYES

Blackman, Kirsty	Davies-Jones, Alex
Bonnar, Steven	Nichols, Charlotte

NOES

Ansell, Caroline	Fletcher, Nick
Bailey, Shaun	Maclean, Rachel
Bristow, Paul	Scully, Paul
Collins, Damian	Wood, Mike

Question accordingly negatived.

New Clause 9

OFFENCE OF FAILING TO COMPLY WITH A RELEVANT DUTY

“(1) The provider of a service to whom a relevant duty applies commits an offence if the provider fails to comply with the duty.

(2) Where the provider is an entity and the offence is proved to have been committed with the consent or connivance of—

- (a) a senior manager or director of the entity, or
- (b) a person purporting to act in such a capacity,

the senior manager, director or person (as well as the entity) is guilty of the offence and liable to be proceeded against and punished accordingly.

(3) A person who commits an offence under this section is liable on conviction on indictment to imprisonment for a term not exceeding two years or a fine (or both).

(4) In this section—

a ‘director’, in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate;

‘relevant duty’ means a duty provided for by section 11, 14, 18, 19, 21 or 30 of this Act; and

‘senior manager’ has the meaning given in section 89(4) of this Act.”—(*Nick Fletcher.*)

Brought up, and read the First time.

Nick Fletcher (Don Valley) (Con): I beg to move, That the clause be read a Second time.

It is a pleasure to serve under your chairmanship, Dame Angela. If you will allow, I want to apologise for comments made on the promotion of suicide and self-harm to adults. I believed that to be illegal, but apparently it is not. I am a free speech champion, but I do not agree with the promotion of this sort of information. I hope that the three shields will do much to stop those topics being shared.

I turn to new clause 9. I have done much while in this position to try to protect children, and that is why I followed the Bill as much as I could all the way through. Harmful content online is having tragic consequences for children. Cases such as that of Molly Russell demonstrate the incredible power of harmful material and dangerous algorithms. We know that the proliferation of online pornography is rewiring children's brains and leading to horrendous consequences, such as child-on-child sexual abuse. This issue is of immense importance for the safety and protection of children, and for the future of our whole society.

Under the Bill, senior managers will not be personally liable for breaching the safety duties, and instead are liable only where they fail to comply with information requests or willingly seek to mislead the regulator. The Government must hardwire the safety duties to deliver a culture of compliance in regulated firms. The Bill must be strengthened to actively promote cultural change in companies and embed compliance with online safety regulations at board level.

We need a robust corporate and senior management liability scheme that imposes 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 the directors and senior

[Nick Fletcher]

managers of financial institutions, and those responsible individuals face regulatory enforcement if they act in breach of such duties.

The Joint Committee on the draft Online Safety Bill, which conducted pre-legislative scrutiny, recommended that a senior manager at or reporting to board level

“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.”

Some 82% of UK adults would support the appointment of a senior manager to be held liable for children’s safety on social media sites, and I believe that the measure is also backed by the NSPCC.

There is no direct relationship in the Bill between senior management liability and the discharge by a platform of its safety duties. The Government have repeatedly argued against the designation of a specific individual as a safety controller for some understandable reasons: an offence could be committed by the company without the knowledge of the named individual, and the arrangement would allow many senior managers and directors to face no consequences. However, new clause 9 would take a different approach by deeming any senior employee or manager at the company to be a director for the purposes of the Bill

The concept of consent or connivance is already used in other Acts of Parliament, such as the Theft Act 1968 and the Health and Safety at Work etc. Act 1974. In other words, if a tech platform is found to be in breach of the Online Safety Bill—once it has become an Act—with regard to its duties to children, and it can be proven that this breach occurred with the knowledge or consent of a senior person, that person could be held criminally liable for the breach.

I have been a director in the construction industry for many years. There is a phrase in the industry that the company can pay the fine, but it cannot do the time. I genuinely believe that holding directors criminally liable will ensure that the Bill, which is good legislation, will really be taken seriously. I hope the Minister will agree to meet me to discuss this further.

1.15 pm

Damian Collins: I want to briefly speak on this amendment, particularly as my hon. Friend the Member for Don Valley referenced the report by the Joint Committee, which I chaired. As he said, the Joint Committee considered the question of systematic abuse. A similar provision exists in the data protection legislation, whereby any company that is consistently in breach could be considered to have failed in its duties under the legislation and there could be criminal liability. The Joint Committee considered whether that should also apply with the Online Safety Bill.

As the Bill has gone through its processes, the Government have brought forward the commencement of criminal liability for information offences, whereby if a company refuses to respond to requests for information or data from the regulator, that would be a breach of their duties; it would invoke criminal liability for a named individual. However, I think the question of

a failure to meet the safety duty set out in the Bill really needs to be framed along the lines of being a systematic and persistent breach, as the Joint Committee recommended. If, for example, a company was prepared to ignore requests from Ofcom, use lawyers to evade liability for as long as possible and consistently pay fines for serious breaches without ever taking responsibility for them, what would we do then? Would there be some liability at that point?

The amendment drafted by my hon. Friend the Member for Stone (Sir William Cash) is based on other existing legislation, and on there being knowledge—with “consent or connivance”. We can see how that would apply in cases such as the diesel emissions concerns raised at Volkswagen, where there was criminal liability, or maybe the LIBOR bank rate rigging and the serious failures there. In those cases, what was discovered was senior management’s knowledge and connivance; they were part of a process that they knew was illegal.

With the amendment as drafted, the question we would have is: could it apply for any failure? Where management could say, “We have created a system to resolve this system that hasn’t worked on this occasion”, would that trigger it? Or is it something broader and more systematic? These failures will be more about the failure to design a regime that takes into account the required stated duties, rather than a particular individual act, such as the rigging of the LIBOR rates or giving false public information on diesel emissions, which could only be made at a corporate level.

When I chaired the Joint Committee, we raised the question, “What about systematic failure, as we have that as an offence in data protection legislation?” I still think that would be an interesting question to consider when the Bill goes to another place. However, I have concerns that the current drafting would not fit quite as well in the online safety regime as it does in other industries. It would really need to reflect consistent, persistent failures on behalf of a company that go beyond the criminal liabilities that already exist in the Bill around information offences.

The Chair: Just to be clear, it is new clause 9 that we are reading a Second time, not an amendment.

Damian Collins: Forgive me, Dame Angela.

Caroline Ansell (Eastbourne) (Con): I rise to recognise the spirit and principle behind new clause 9, while, of course, listening carefully to the comments made by my hon. Friend the Member for Folkestone and Hythe. He is right to raise those concerns, but my question is: is there an industry-specific way in which the same responsibility and liability could be delivered?

I recognise too that the Bill is hugely important. It is a good Bill that has child protection at its heart. It also contains far more significant financial penalties than we have previously seen—as I understand it, 10% of qualifying revenue up to £18 million. This will drive some change, but it comes against the backdrop of multi-billion-pound technology companies.

I would be interested to understand whether a double lock around the board-level responsibility might further protect children from some of the harrowing and harmful content we see online. What we need is nothing short of

transformation and significant culture change. Even today, *The Guardian* published an article about TikTok and a study by the Centre for Countering Digital Hate, which found that teenagers who demonstrated an interest in self-harm and eating disorders were having algorithms pushing that content on to them within minutes. That is most troubling.

We need significant, serious and sustained culture change. There is precedent in other sectors, as has been mentioned, and there was a previous recommendation, so clearly there is merit in this. My understanding is that there is strong public support, because the public recognise that this new responsibility cannot be strengthened by anything other than liability. If there is board-level liability, that will drive priorities and resources, which will broker the kind of change we are looking for. I look forward to what the Minister might share today, as this has been a good opportunity to bring these issues into further consideration, and they might then be carried over into subsequent stages of this excellent Bill.

Rachel Maclean (Redditch) (Con): I would like to build on the excellent comments from my colleagues and to speak about child sexual abuse material. I thank my hon. Friends the Members for Penistone and Stocksbridge (Miriam Cates) and for Stone for tabling the amendment. I am very interested in how we can use the excellent provisions in the Bill to keep children safe from child sexual abuse material online. I am sure the Committee is aware of the devastating impact of such material.

Sexual abuse imagery—of girls in particular—is increasingly prevalent. We know that 97% of this material in 2021 showed female children. The Internet Watch Foundation took down a record-breaking 252,000 URLs that had images of children being raped, and seven in 10 of those images were of children aged 11 to 13. Unfortunately, the National Crime Agency estimates that between 550,000 and 850,000 people in the UK are searching for such material on the internet. They are actively looking for it, and at the moment they are able to find it.

My concern is with how we use what is in the Bill already to instil a top-down culture in companies, because this is about culture change in the boardroom, so that safety is considered with every decision. I have read the proceedings from previous sittings, and I recognise that the Government and Ministers have said that we have sufficient provisions to protect children, but I think there is a little bit of a grey area with tech companies.

I want to mention Apple and the update it was planning for quite a few years. There was an update that would have automatically scanned for child sex abuse material. Apple withdrew it following a backlash from encryption and privacy experts, who claimed it would undermine the privacy and security of iCloud users and make people less safe on the internet. Having previously said that it would pause it to improve it, Apple now says that it has stopped it altogether and that it is vastly expanding its end-to-end encryption, even though law enforcement agencies around the world, including our own UK law enforcement agencies, have expressed serious concerns because it makes investigations and prosecution more challenging. All of us are not technical experts. I do not believe that we are in a position to judge how

legitimate it is for Apple to have this pause. What we do know is that while there is this pause, the risks for children are still there, proliferating online.

We understand completely that countering this material involves a complicated balance and that the tech giants need to walk a fine line between keeping users safe and keeping their data safe. But the question is this: if Apple and others continue to delay or backtrack, will merely failing to comply with an information request, which is what is in the Bill now, be enough to protect children from harm? Could they delay indefinitely and still be compliant with the Bill? That is what I am keen to hear from the Minister. I would be grateful if he could set out why he thinks that individuals who have the power to prevent the harmful content that has torn apart the lives of so many young people and their families should not face criminal consequences if they fail to do so. Can he reassure us as to how he thinks that the Bill can protect so many children—it is far too many children—from this material online?

Alex Davies-Jones: Labour supports new clause 9, as liability is an issue that we have repeatedly raised throughout the passage of the Bill—most recently, on Report. As colleagues will be aware, the new clause would introduce criminal liabilities for directors who failed to comply with their duties. This would be an appropriate first step in ensuring a direct relationship between senior management of platforms and companies, and their responsibilities to protect children from significant harm. As we have heard, this measure would drive a more effective culture of awareness and accountability in relation to online safety at the top of and within the entire regulated firm. It would go some way towards ensuring that online safety was at the heart of the governance structures internally. The Bill must go further to actively promote cultural change and put online safety at the forefront of business models; it must ensure that these people are aware that it is about keeping people safe and that that must be at the forefront, over any profit. A robust corporate and senior management liability scheme is needed, and it needs to be one that imposes personal liability on directors when they put children at risk.

The Minister knows as well as I do that the benefits of doing so would be strong. We have only to turn to the coroner's comments in the tragic case of Molly Russell's death—which I know we are all mindful of as we debate this Bill—to fully understand the damaging impact of viewing harmful content online. I therefore urge the Minister to accept new clause 9, which we wholeheartedly support.

Paul Scully: The Government recognise that the intent behind the new clause is to create new criminal offences of non-compliance with selected duties. It would establish a framework for personal criminal offences punishable through fines or imprisonment. It would mean that providers committed a criminal offence if they did not comply with certain duties.

We all want this Bill to be effective. We want it to be on the statute book. It is a question of getting that fine balance right, so that we can properly hold companies to account for the safety of their users. The existing approach to enforcement and senior manager liability strikes the right balance between robust enforcement and deterrent, and ensuring that the UK remains an attractive place to do business. We are confident that

[Paul Scully]

the Bill as a whole will bring about the change necessary to ensure that users, especially younger users, are kept safe online.

This new clause tries to criminalise not complying with the Bill's duties. Exactly what activity would be criminalised is not obvious from the new clause, so it could be difficult for individuals to foresee exactly what type of conduct would constitute an offence. That could lead to unintended consequences, with tech executives driving an over-zealous approach to content take-down for fear of imprisonment, and potentially removing large volumes of innocuous content and so affecting the ability for open debate to take place.

Kirsty Blackman: Does the Minister not think that the freedom of speech stuff and the requirement to stick to terms of service that he has put in as safeguards for that are strong enough, then?

Paul Scully: I come back to this point: I think that if people were threatened with personal legal liability, that would stifle innovation and make them over-cautious in their approach. That would remove the balance, disturb the balance, that we have tried to achieve in this iteration of the Bill. Trying to keep internet users, particularly children, safe has to be achieved alongside free speech and not at its expense.

Further, the threat of criminal prosecution for failing to comply with numerous duties also runs a real risk of damaging the attractiveness of the UK as a place to start up and grow a digital business. I want internet users in the future to be able to access all the benefits of the internet safely, but we cannot achieve that if businesses avoid the UK because our enforcement regime is so far out of kilter with international comparators. Instead, the most effective way to ensure that services act to protect people online is through the existing framework and the civil enforcement options that are already provided for in the Bill, overseen by an expert regulator.

1.30 pm

Going forward, companies will need to regularly assess the risks that their services pose to users, including ahead of any major design or functionality changes, and put in place proportionate systems and processes to mitigate those risks. It is only when companies thoroughly understand the risks arising from their services that they will be able to take proportionate action to keep users safe. This approach will fundamentally change the way tech services operate. It will mandate that services and tech executives properly consider risks and user safety from the get-go, rather than as an afterthought once a product is already open to users.

If platforms fail to comply with their enforceable requirements, Ofcom will be able to use its range of strong enforcement powers, including fines. By court order, it will be able to take business disruption measures and block sites from operating in the UK. Make no mistake about the substance of those fines: it is 10% of a company's global turnover. No matter how big the company is, 10% is 10%; it is still a massive proportion of operating costs that will be removed. Our approach will ensure that providers are held to account and that swift action is taken to keep users safe, whether by bringing the platform into compliance or through stronger measures.

Senior tech executives can already be held criminally liable under the Bill for failing to take reasonable steps to ensure their company properly complies with Ofcom's information requests. That includes failing to ensure that their company responds fully, accurately and on time; failing to ensure that their company does not provide false information; failing to ensure that their company does not provide encrypted information that Ofcom cannot understand; and failing to ensure that their company does not destroy or alter information required by Ofcom.

If we start to widen the scope of senior management liability in the Bill, we start to come up against problems quickly. For a criminal offence, a precise statement of the prohibited behaviour must clearly be set out—in other words, that a particular act or omission constitutes the criminal offence. In this case, a failure to comply with the relevant duties listed in the amendment would depend on a huge number of factors. That is because the Bill applies to a providers of various sizes and types. In most areas, the framework is flexible, rather than prescriptive: it does not prescribe certain steps that providers must take. That means that it may be difficult for individuals to foresee exactly what type of conduct constitutes an offence, and that can easily lead to unintended consequences and to tech executives taking an over-zealous approach to content take-down for fear of imprisonment.

My hon. Friend the Member for Folkestone and Hythe talked about health and safety, LIBOR and diesel emissions, which have been raised here and in the main Chamber. There is a big difference between what we are talking about and those examples. On health and safety, LIBOR and the cover-up of diesel emissions, there is far closer contact with a personal conduct measure; the Bill contains broader measures.

My hon. Friend the Member for Eastbourne talked about having an industry-specific way of delivering the responsibility and liability. This is the industry-specific way. We are making sure that the approach is proportionate and that executives have to co-operate with Ofcom at every stage. It is pre-emptive as well as reactive. It ensures that that, when Ofcom assesses their risk assessments, their approaches to algorithms and so on, it has all the facilities it needs to check that what they are doing is the right approach. If there are complaints and systemic failings within the platform's regime, they need to comply; they must not cover it up or hinder Ofcom's investigation.

On the TikTok algorithm, the development of an algorithm is quite remote from personal conduct. It is not easy to make an individual criminally liable for it, not least because algorithms tend to be developed by hundreds if not thousands of people in different continents. To boil that down to one person is incredibly difficult.

We also heard about the example of Apple. There is no way that through this legislation, we are banning, or creating back doors in, end-to-end encryption; there is no safe back door, frankly, so if we did that, we could kiss goodbye to open banking and any number of things that we use daily. I may be wrong, but my understanding of the Apple product that was mentioned is that it would involve scanning pretty well everything that a person had in their iCloud, so it would be a sledgehammer to crack a nut, although clearly a really important nut. If Apple will not bring that forward, we

would expect it and other platforms to bring forward something else that is effective specifically against terrorism content and child sexual exploitation and abuse.

For the reasons that I have given, I strongly believe that the Bill's approach to enforcement will be effective. It will protect users without introducing incentives for managers to remove swathes of content out of fear of prosecution. I want to make sure that the legislation gets on the books and is proportionate, and that we do not start gold-plating it with these sorts of measures now, because we risk disrupting the balance that I think we have achieved in the Bill as amended.

Nick Fletcher: I appreciate the Minister's comments, but from what my hon. Friends the Members for Folkestone and Hythe, for Eastbourne, and for Redditch said this morning about TikTok—these sorts of images get to children within two and a half minutes—it seems that there is a cultural issue, which the hon. Member for Pontypridd mentioned. Including new clause 9 in the Bill would really ram home the message that we are taking this seriously, that the culture needs to change, and that we need to do all that we can. I hope that the Minister will speak to his colleagues in the Ministry of Justice to see what, if anything, can be done.

Paul Scully: I forgot to respond to my hon. Friend's question about whether I would meet him. I will happily meet him.

Nick Fletcher: I appreciate that. We will come back to this issue on Report, but I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

Question proposed, That the Chair do report the Bill, as amended, to the House.

The Chair: It is usual at this juncture for there to be a few thanks and niceties, if people wish to give them.

Paul Scully: I apologise, Dame Angela; I did not realise that I had that formal role, but you are absolutely right.

The Chair: If the Minister does not want niceties, that is up to him.

Paul Scully: Dame Angela, you know that I love niceties. It is Christmas—the festive season! It is a little bit warmer today because we changed room, but we remember the coldness; it reminds us that it is Christmas.

I thank you, Dame Angela, and thank all the Clerks in the House for bringing this unusual recommittal to us all, and schooling us in the recommittal process. I

thank Members from all parts of the House for the constructive way in which the Bill has been debated over the two days of recommittal. I also thank the Doorkeepers and my team, many of whom are on the Benches here or in the Public Gallery. They are watching and WhatsApping—ironically, using end-to-end encryption.

The Chair: I was just about to say that encryption would be involved.

Paul Scully: I look forward to continuing the debate on Report.

Alex Davies-Jones: I thank you, too, Dame Angela. I echo the Minister's sentiments, and thank all the Clerks, the Doorkeepers, the team, and all the stakeholders who have massively contributed, with very short turnarounds, to the scrutiny of this legislation. I have so appreciated all that assistance and expertise, which has helped me, as shadow Minister, to compile our comments on the Bill following the Government's recommittal of it to Committee, which is an unusual step. Huge thanks to my colleagues who joined us today and in previous sittings, and to colleagues from across the House, and particularly from the SNP, a number of whose amendments we have supported. We look forward to scrutinising the Bill further when it comes back to the House in the new year.

Kirsty Blackman: I thank you, Dame Angela, as well as Sir Roger for chairing our debates. Recommittal has been a very odd and unusual process; it has been a bit like groundhog day, discussing things we have discussed previously. I very much appreciate the hard work of departmental and Ofcom staff that went into making this happen, as well as the work of the Clerks, the Doorkeepers, and the team who ensured that we have a room that is not freezing—that has been really helpful.

I thank colleagues from across the House, particularly the Labour Front-Bench spokespeople, who have been incredibly helpful in supporting our amendments. This has been a pretty good-tempered Committee and we have all got on fairly well, even though we have disagreed on a significant number of issues. I am sure we will have those arguments again on Report.

The Chair: There being no more obvious niceties, I add my thanks to everybody. I wish everybody season's greetings and a happy Christmas.

Question put and agreed to.

Bill, as amended, accordingly to be reported.

1.41 pm

Committee rose.

Written evidence reported to the House

OSB113 HOPE not hate

OSB114 Samaritans

OSB115 Jeffrey Howard, Associate Professor of Political Theory and Director of the Online Speech Project, School of Public Policy, University College London

OSB116 Open Rights Group

OSB117 Meta

