



Communications & Digital Committee

Corrected oral evidence: Online Safety Bill

Tuesday 6 December 2022

2.30 pm

[Watch the meeting](#)

Members present: Baroness Stowell of Beeston (The Chair); Baroness Bull; Baroness Featherstone; Lord Foster of Bath; Lord Griffiths of Burry Port; Lord Hall of Birkenhead; Lord Lipsey; Lord Vaizey of Didcot; The Lord Bishop of Worcester; Lord Young of Norwood Green.

Evidence Session No. 1

Heard in Public

Questions 1 - 12

Witnesses

I: Professor Lorna Woods, Professor of Internet Law, Essex Law School, University of Essex; Richard Collard, Policy and Regulatory Manager, Child Safety Online, NSPCC; Matthew Feeney, Head of Tech & Innovation, Centre for Policy Studies; Dr Edina Harbinja, Reader in Media/Privacy Law, Aston Law School, Aston University.

USE OF THE TRANSCRIPT

This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Examination of witnesses

Professor Lorna Woods, Richard Collard, Matthew Feeney and Dr Edina Harbinja.

Q1 The Chair: This is the Communications and Digital Committee. We are having a special session on the Online Safety Bill. Welcome to our witnesses. I will ask them to introduce themselves in a moment. The committee did an inquiry into freedom of speech online a couple of years ago and published a report in summer 2021. We said that we would return to the Online Safety Bill once we expected it to come to the House of Lords, so this is a session we were intending to have in any case. Since then, of course, the Government decided to pause the progress of the legislation and then withdraw it, and they intend to make some changes to it. They reintroduced it yesterday and we are expecting it to arrive in the House of Lords in January.

I am pleased to have before us four witnesses who I think have different perspectives on the legislation. We are looking forward to hearing their views on the Bill and the changes the Government have made to it. The committee will consider their contributions today. We also aim to have a session with Ministers in the new year. We will then consider how best to use the information we have heard in how we assist the work of the House of Lords. I ask the witnesses to introduce themselves.

Dr Edina Harbinja: I am a reader in law at Aston University. This is my second time in front of the committee. I was part of the free speech online inquiry. I also gave oral evidence to the Joint Committee on the Draft Online Safety Bill and the DCMS Committee in the Commons. So I am quite experienced with the Bill and its progress. Thank you for this opportunity.

Professor Lorna Woods: I am professor of internet law and a member of the Human Rights Centre at the University of Essex. I have been in the field of communications regulation since the Broadcasting Act 1990. I have been working with the Carnegie UK Trust. It was on the basis of my research that we got the systemic approach and the duty of care, which I think inspired the online harms White Paper. So I too am familiar with the Bill.

Matthew Feeney: I am the head of technology and innovation at the Centre for Policy Studies. I moved back to London in July after 10 years living in Washington DC or the DC area. I was formerly the director of the Cato Institute's project on emerging technologies, where I worked on, among other things, online speech issues.

Richard Collard: I am from the NSPCC. We are the organisation that originally won the commitment from government to regulate and stop online harms to children.

Q2 The Chair: You are all very welcome. We will cover four main areas in our questions today. I will categorise them as adults, children, any gaps you perceive in the legislation as it now stands, and, finally—the last two overlap a bit—the amendments we are expecting to arrive in the House

of Lords or where you think there might be a particular focus on amendments.

I will kick off with an open question. Starting with “legal but harmful”—the topic that has been the main focus of the Government’s changes to this legislation—I am interested in hearing your views, that element of the Bill having been removed, on the balance between freedom of speech and the protection of adults; we will come to children later. I just wanted to start on that main balance between freedom of speech and the general protection of people online.

Dr Edina Harbinja: Thank you for the question. Although I did argue that the “legal but harmful” content should be dropped from the Bill and I can applaud that suggestion, I do not think it shifts the balance significantly in favour of free speech—

The Chair: You do not?

Dr Edina Harbinja: I do not, no. I do not think the balance is quite right. There are some major concerns about the implications of the current version, whatever it is—we are told that there are amendments, and in one of the versions that was published today there were further amendments, to the Bill. There is concern, first, about how content that is harmful to children will impact adults and be policed by the companies, and whether that would create an incentive for the companies to protect their services and networks more, even if they are not targeting children particularly, just to be on the safe side and to comply with that duty. That is one concern.

The second concern relates to offences, some of which will be removed, as we have heard, such as the harmful communications one. The false communications offence, the threatening communications offence and further offences added to the Bill, again, raise major concerns about the Bill. That is in tandem with the obligation on illegal content, where the companies will need to judge illegality. The standard in the Bill at the moment in new Clause 166 is “reasonable grounds to infer” illegality. This is a very problematic standard. It is contrary to the established standard of “manifest illegality” and it is really difficult to understand how companies could apply this standard in practice. Of course, Clause 167 mandates that Ofcom will produce some guidance on this but, again, Ofcom, as a regulator, is not in a position to do this and decide on this very important question when it comes to illegality and the standard that is ab initio inadequate, in my opinion.

The Chair: Professor Woods, what is your overall view on the balance now following these changes?

Professor Lorna Woods: I should probably start by saying that I thought that the claims about freedom of expression in the first place were overstated and underevidenced and seemed to bear little relationship to the European convention court’s jurisprudence as a whole.

In so far as the majority of campaigning materials referred to case law, it was isolated and pick-and-mix style. I question whether there was a problem in the first place, because the original duty essentially required

transparency rather than a duty to take down. There was a lot of misreporting in the media last week, so I emphasise that point.

There is an issue. On the one hand, it would be nice if the companies enforced their terms of service. It would be a very helpful step forward. Unfortunately, the way it is drafted, there is no minimum. I do not know what modelling DCMS did to see whether there were any perverse incentives to make terms of service so long and complex that they became unworkable or there was any downward pressure. It is not a good analogy because the circumstances are perhaps unique, but we saw that with Twitter removing chunks of its policies in the last few weeks. There are examples of Facebook withdrawing its policy on slave trading in the Middle East because it affected companies' profitability. There is a risk there that we might end up in some strange places.

I also wonder whether this focuses too much on the relationship between the user and the terms of service and less on design issues. That is what the systems approach was originally about. Those issues were raised by the joint scrutiny committee and by this committee in its previous reports about design and the role of algorithms. Here, this is just about policing users and not so much about encouraging good design.

That is seen particularly with the removal of the risk assessment obligation and the obligation to publish a summary. The risk assessment would allow users to get a sense of what the platform was like so that they could make an informed choice about whether they wanted to engage with it. That has gone, but if we are expecting to rely on user empowerment tools, which in principle are a good thing, surely we want users to know what they are engaging with to start with. There is a problem there with the loss of the risk assessment and of the requirement to summarise that risk assessment and make it public.

I have one final point about the risk assessment. The user empowerment tools are required to be effective, but how will we know if they are effective if we do not know about any of the prevailing conditions on the platform? That sort of transparency has been lost in this set of amendments. There is a greater risk, perhaps, than under the previous situation.

We have not yet seen the amendments—or maybe they are in the most recent version and I have not caught up with it—about Ofcom and its risk assessment and risk profiles, and the extent to which Ofcom will pick that up. Without an obligation it will be quite difficult to do a risk assessment on the companies.

The Chair: Mr Feeney, so far we have had a “not improved” and a “got worse”. What is your verdict?

Matthew Feeney: After looking at the revised Bill with the amendments, the thrust of free speech remains about the same. The removal of the “legal but harmful” content provision was welcome, but the Bill still includes duties for the protection of children, which, although a laudable goal, require firms to moderate content in much the same

way as they would have had to deal with what was called “legal but harmful”.

I agree with Professor Woods that the reporting on that was rather poor. Although the Government portrayed the provision as a transparency requirement, it is unlikely that the major firms that are often discussed in this context—the Facebooks, Googles and Twitters of the world—would have taken the step either to do nothing or to promote the content in question and would have, in the light of that, engaged in overmoderation of legal content. There is an important, linked issue associated with encryption that perhaps might be for further discussion, but I think those who are worried about the state of free speech will have welcomed the revision to “legal but harmful”, although there are still threats.

The Chair: Do you think it is possible to protect freedom of speech while introducing some provisions to protect children? You referred to the fact that “legal but harmful” still applies to children. Do you think it is possible to do both at the same time?

Matthew Feeney: It would be very difficult, in part because of the nature of how the internet works. It is very difficult for anyone snooping on a network to know whether data is being accessed by a child or by an adult. Therefore, it would be rational for an online firm in this legal environment to err on the side of caution and assume that all users are children. Given the potential fines and the implications of infringement, that is what would happen. I hesitate to say that it would be impossible, because I am not an engineer and there might be ways to do it, but at best it is very difficult.

The Chair: It is one of those things where there are trade-offs, as it were.

Matthew Feeney: Of course, and maybe they are worth it. That is for lawmakers to decide.

The Chair: Mr Collard, as I said, we will come to the specific issues of child protection a bit later, but give us your view on how the balance of the Bill sits now.

Richard Collard: Obviously, the NSPCC’s position is on preventing abuse to children, but we think the balance is in the right place at the moment. The previous version of the Bill also had the balance in the right place. We need to remember that a fifth of all internet users in the UK are children and they have the right to freedom of speech but also to safety. Although the adult safety duties have been removed, we are pleased and reassured that the child safety duties are staying within the Bill’s scope, because that will create a systemic approach to protecting children from harm.

I will quickly touch on what harm looks like in this case. Obviously, in the last few months we saw the damage done by harmful content played to Molly Russell, who was bombarded with self-harm and suicide content and took her own life. We need to remember that this harm is not an individual case. Last year, the NSPCC’s Childline delivered 24,000 counselling sessions to children who had suicidal thoughts. All too often

they told us about how this harmful content is shown to them. It is not something that they seek out; it is algorithmically designed to go to them. That is how the business models of these platforms work. It is really important that we take a systematic approach, not a content-based approach. We are really happy that the duty of care framework is in place.

The Chair: Would it be fair to say, then, that so far we have had from Dr Harbinja that the changes have not improved the Bill, from Professor Woods a sense that things have got worse, from Mr Feeney that it is probably about the same and that things have not necessarily improved but it is an improvement that “legal but harmful” is not part of the picture, and that the NSPCC thinks that it is okay?

Richard Collard: I think the balance is in the right place. There are some implications of removing “legal but harmful” to adults that will impact on children. I believe that we have time to go into those implications later, but I can go into them now, if that is helpful.

Q3 **The Chair:** We will come on to those in a moment. I have one further question concerning the reference to illegal content. Do you want to raise anything about the requirements for companies having to proactively monitor or prevent users from encountering priority illegal content?

Dr Edina Harbinja: Yes, thank you for the question. Clause 106—it was previously Clause 104—is about the notices to deal with terrorist and CSEA content, and the use of accredited technology to identify this content shared publicly or privately. This is where we fear that end-to-end encryption would be compromised with these notices from Ofcom, especially in the private communication channels. Also, when we talk about the user base, most of us, about 40 million UK residents, use WhatsApp. Compromising encrypted communications—essentially mandating the client-side scanning or the communication—is not a proportionate step.

I respectfully disagree with Professor Woods on the European Convention on Human Rights. We have very clear evidence in the caseload that this Bill, and guidance from Ofcom regarding different aspects of free speech, including judging illegality, does not meet the threshold of limiting free speech under the convention and Article 10, because it is not prescribed in law. A lot of that is prescribed by the regulator. It is discretion in the guidance, not law. Also, a lot of that is not certain, proportionate or necessary in a democratic society. I counter the argument that the European Convention on Human Rights has not been considered.

The Chair: I do not want this to turn into a debate among our witnesses about the pros and cons of human rights law.

Professor Lorna Woods: I have two points. A lot of convention case law says that codes and the like can count as the law for the purposes of the convention. You see this particularly in the surveillance case law when the codes have not even been particularly well published.

Regarding the concern about criminal content and too much coming down, paragraph 106 of the judgment in *Animal Defenders International v United Kingdom* states that “a state can, consistently with the convention, adopt general measures which apply to pre-defined situations regardless of the individual facts of each case even if this might result in individual hard cases. Contrary to the applicant's submission, a general measure is to be distinguished from a prior restraint imposed on an individual act of expression”.

That tells us that we can have general rules, even if they may not be perfect.

The Chair: You have illustrated how much enjoyment our legal colleagues will have when this legislation arrives in the House of Lords.

- Q4 **Lord Lipsey:** I started off being in favour of the “legal but harmful” provisions in the original Bill. Therefore, I am weighing quite carefully the substitute in this Bill. However, the more I think about it, the more bizarre it seems. This Bill relies on users blocking themselves off from harmful content. If I do not want to commit suicide, I might well do that, but it would not be a great gain. However, if I did want to commit suicide, I would want as much suicide content as I could get.

I am bemused as to why this is felt to be a good substitute for “legal but harmful”, because if there is no good substitute. we might go back to that.

The Chair: Is that a comment rather than a question?

Lord Lipsey: It was meant to have an interrogative note.

Lord Vaizey of Didcot: It was a question in seminar style.

The Chair: Maybe that is one for Mr Feeney to respond to.

Matthew Feeney: Maybe. I will try. Perhaps I spent too long in the United States, but the very concept of “legal but harmful” struck me as somewhat strange to begin with. I urge lawmakers to consider that, often in these discussions, it is the context of content that matters rather than the content itself. The harm of content is often associated with where it is seen and in what context.

Some of the larger social media firms emphasise, with their own harmful-content policies, the context in which that content will be allowed. Other than with content that is illegal by definition, such as child sexual abuse imagery, the context is the determining factor. That must be appreciated as the Bill is debated.

- Q5 **The Lord Bishop of Worcester:** Thank you very much indeed for being with us and helping us with this. As you know, we have deliberated long about this matter and have been grateful for help in the past.

We have looked at children generally, but I now want to focus on this. Are the provisions for protecting children online adequate, or do they need to be strengthened further?

Richard Collard: If we take a step back and remember why the Bill was introduced, it was to ensure that children could go online and be safe. That should be a fundamental value that we respect throughout this. Looking at the backdrop of where we are today, we have online grooming at an all-time high, up by 84% in the last four years. We estimate that on average there are 100 child online sex crimes occurring in the UK every day. We have also recently heard from a coroner who concluded that social media firms contributed to the death of a child.

Our red lines and our focus on the Bill are clear. It must tackle preventable child abuse, it must stop harm to children, and it must work in practice. Our assessment is that the duty-of-care approach and the child safety duties, along with the legal safety duties, will create this risk-based and systematic approach that will protect children. Technology companies will be forced to disrupt child abuse, whether it occurs in public spaces or in private messaging. That is really important. It will disrupt upstream abuse—how abusers organise online to commit abuse—and do so in a systematic way that also protects children from harmful content.

There are two main areas, though, where the Bill needs to be strengthened. First, it needs to ensure that user advocacy arrangements are in place in the Bill. In other regulatory regimes—energy, water, transport—there are user advocate organisations. They are set up by the Government to play a role as an independent champion of user interests in complex regulatory regimes. Citizens Advice is the most obvious example; it plays that role of championing the voice of consumers.

In the case of the online safety regime, we think it is really important that children have a voice in this debate, because a lot of the time these platforms do not listen to the voice of children, and this is why we need to regulate in the first place.

Secondly, having a user advocate will provide an early-warning function. It will be able to find new and emerging risks to children and raise that with the regulated companies. Thirdly, it is about balancing out against big tech.

Ofcom will play a role as an independent regulator that will be evidence-based, but the tech companies will be looking to hire policy professionals and legal professionals and commission research that will make their case that abuse is not so bad at the moment and that perpetration is down, and to try to avoid their regulatory obligations. There needs to be a counterbalance to that.

Most of all, it is really important that children have a voice, because this is something that they want. We at the NSPCC hosted an event in the Lords last weekend which I know a number of committee members attended. It was an opportunity for children to explain why they felt that their needs have to be reflected in the Bill. They subsequently sent a letter to Michelle Donelan saying that the people in charge of making the Bill happen have not grown up with the internet as they have, so would not know what it was like to navigate it as a young person, and therefore that young people should be at the forefront of decision-making because

they are the experts in their own lives. That is really powerful and shows that children really want this regime to work and want to protect it, but they know that their needs have to come first.

The second area where the Bill needs to be strengthened is in providing Ofcom with the powers it needs to get compliance from the tech companies. We want to see senior-manager responsibility and liability in the Bill. It was all too clear from the case of Molly Russell that the executives at Meta have a fundamental disconnect between what they think is safe and what parents in the UK think is safe. Ian Russell said that the only person in the world since Molly's death who thought the content she had viewed was safe for her was the head of health and well-being at Meta. We think there need to be powers in the Bill that name an individual in a tech company who is responsible for child safety so that it is a compliance matter that flows down and culture changes in those companies, which can then be held responsible for grievous failures to children.

Matthew Feeney: As I mentioned in answer to your previous question, I would like the Bill to account for the context of a lot of the content. While we might seek to educate children about the risks of online behaviour, sometimes content that is designated as harmful might be useful for an educational purpose.

I would add that a few years ago Apple was interested in implementing a method by which parents of children who had received sexually explicit imagery or other offensive content could be automatically notified. I mention that, because there are online firms or tech companies that are trying to figure out ways in which children can learn more about dangerous content but also allow for their close family members to be informed. However, it is important to consider that—as Mr Collard and his colleagues know all too well—oftentimes family members are, regrettably, the perpetrators of abuse against children, and any legislation dealing with this kind of content should make sure to mention explicitly that parental notification of child receipt of this kind of content is not necessarily obliged. That is one of the nuances that are often missed.

Those are the first two thoughts that occur to me in response to your question.

Professor Lorna Woods: I defer to the NSPCC on matters relating to children. I will say that the way the Bill is and was means that there is a steep drop-off when someone hits 18; they go from protected to unprotected, and I am not sure that is wise.

To return to Lord Lipsey's point, there may be another alternative, which is that user-empowerment tools could be switched on by default. That is not a complete solution, but it would mitigate some of the concerns.

Dr Edina Harbinja: I second what Mr Feeney has said. I would add that in the media, and often in Parliament, we get the impression that we are talking about an online children's safety Bill or a Bill that aims to publish

punish big-tech bosses. That is the narrative that we see quite a lot in the media, and it is wrong because the Bill goes far beyond that.

We all acknowledge that the aim to protect children is essential and legitimate, but the way the Bill is drafted goes far beyond that and potentially impacts, for example, 25,000 small and medium-sized businesses that have nothing to do with Meta, Google, Twitter or Elon Musk but will have to comply with the Bill. It poses a threat to encryption and the security of the internet and of the networks that we all rely on in our day-to-day activities—communication, banking and so on—so that is another impact to consider rather than focusing on the narrative of just protecting children.

It adds areas that were not initially announced in the online harms White Paper. It seems that whenever something pops up in media discourse as an issue in society, , such as immigration, asylum and self-harm, it is added to the Bill. Quite a few new criminal offences have been proposed or added in government amendments to the Bill. So it is not just about protecting children or punishing big tech companies. It goes far beyond impacting businesses and competition; it also impacts the human rights of adults and children—freedom of expression and privacy of both adults and children.

Q6 Lord Young of Norwood Green: Does the removal of the “legal but harmful” provision for adults negatively affect protections for children? I have a couple of comments to make on that. I presume that a lot of this is monitored by algorithms. If I have got that wrong, no doubt you can educate me.

The other question that crosses my mind is: how do you know that children are the age they say they are? Is it possible to have an effective check on age? I am deeply sceptical of that, knowing the ingenuity of children who want to access content.

Richard Collard: Ultimately, removing adult “legal but harmful” changes the burden on regulated companies. Although this is a bit of a caricature, previously they had to protect everyone from harm, but now they just have to protect children from illegal content, harmful content and the illegal safety duties. They can reduce their terms of service; they can water them down so that they do not have to protect adults as much as they previously did. There is much more of a cost on platforms to protect children now.

We think there will be some scenarios that follow logically from that. Some platforms will continue to serve both adults and children, and they will have a divide because they know they have to make sure that children specifically are not shown content that is harmful to them. There are other scenarios that involves platforms saying, “You know what? We’re just not going to serve children anymore, because it’s too costly”, and providing 18-plus services. They might be able to reduce their terms of service and provide adults with harmful content, which is fine according to the Bill, while some platforms might decide just to serve children and spend their entire time serving that pool of people.

That brings additional risks that were not foreseen when the Government decided to take out “legal but harmful” for adults. It essentially places a significant burden on age-assurance technology. I agree with you that it puts a lot on the platforms to find technologies that can identify who is a child and who is an adult. We know today that these tools are not 100% effective, so there will be children who fall through the gap. That means there will be children who end up in areas of the internet designed for adults, with adult content, and they will be subjected to that. There is another perverse consequence, which is that there will be adults who are perpetrators of abuse who try to get into areas of the internet that are designed for children because they see it as a pool of victims who they can attempt to groom. So we need to make sure, if we are going to rely heavily on age assurance, that minimum standards are built into the regimes. We want to see Ofcom given the powers to set minimum standards for age assurance so that it can be effective and protect privacy.

The other thing we want to see is the removal of the children’s access assessment. Platforms will be expected to protect children only if there is a significant number of children on the platform. That gives an out to some problematic platforms, such as Onlyfans or Telegram, which might be able to claim that there should not be a significant number of children on their platform. We want to see the Bill say, “There are a number of children on that platform”, so they would be in line for their regulatory obligations to protect children.

Matthew Feeney: You are correct to point out that, at scale, algorithms are doing a lot of the work. That is a feature of the scale of content. To give a few examples, I think a few years ago it was noted that 500 hours of content are uploaded to YouTube every minute, about 6,000 tweets are uploaded every second, and every day hundreds of millions of photos are uploaded to Facebook. It is a scale of content for which human moderation is just not feasible, so algorithms are often deployed to remove content. There are false positives and false negatives in their process; the history of the internet is full of them.

Age assurance is a difficult issue, because to protect privacy the mechanism, almost by definition, has to be relatively weak. We all know of the banners that appear on some websites that say, “You promise that you are over 18”, or that you are over a certain age, and you just click. That is doing nothing to assure anyone that the visitor to the site is telling the truth. The problem is that the privacy implications become more and more severe the more details you ask users to reveal. People do not like the idea of online firms or their Government knowing intimate details about where they are surfing the web.

I conclude by saying that children are pretty smart. If there is an age-assurance regime that requires the uploading of certain documents, we can expect copies of documents to proliferate for children to upload. I have been told that underage drinkers in the United States, for example, might use fake drivers’ licences to get alcohol. These things happen. There is a difficult balance, though, between how effective you want age assurance to be and how much privacy you want to protect.

Q7 **Baroness Bull:** Professor Woods, you mentioned the cliff edge at the age of 18. I am concerned that it is a ravine, because although the Bill has protections for adults and very specific protections for children, there is an absence of any particular protections for vulnerable adults. I know that is an ill-defined term, or that it is defined in different ways, but I want to ask about two specific categories of vulnerability.

One relates to eating disorders. There is still a concern among the eating disorder community that the amendments do not go far enough to protect people who are at risk of or who have eating disorders. They would argue that content that directly encourages eating disorders meets the same threshold as content that encourages self-harm and so should be banned, but it will not necessarily be because, as Mr Feeney pointed out, that is a different context and the content does not always look as harmful as it actually is. It is sometimes created by people with eating disorders, so we risk criminalising people who are in fact vulnerable.

My second category, which Professor Woods and I have discussed before, is adults with autism, learning disabilities or questions about their mental capacity for whom online is really important, given that this is an isolated community that spends less time outside the home but who have particular risks from being online. Charities saw "legal but harmful" as a way of tackling this, so there is some concern, particularly from Mencap, that that has gone. Lord Lipsey mentioned part of the triple shield, but it is not clear how content that is abusive towards disabilities would be regulated and monitored, and what that would look like. The accessible filters might not be accessible to people with learning disabilities. They do not fall into the children bracket, and nor should they, but they will not be covered in the way that other parts of the community are.

I will start with Professor Woods, because we have talked about this before. Do you share my concerns that the Bill does not adequately cover vulnerable adults, particularly adults with learning disabilities and autism? If so, what could be done to strengthen its provisions so that this community is protected?

Professor Lorna Woods: I have concerns about the coverage. We have an amendment that requires terms of service to be enforced effectively. That depends on what the terms of service say. There is no obligation to cover these issues or to have in mind communities of users when drafting terms of service. You could have a one-size-fits-all approach. Vulnerable adults, in their many manifestations, have not really had much of a look-in in the discussion, which is heavily children/adults, as though all adults are the same.

The user-empowerment tools cover some aspects of vulnerability. A government amendment refers to promotion or "provides instructions for ... suicide or an act of deliberate self-injury, or ... an eating disorder or behaviours associated with an eating disorder", which covers some of the ground but not all the issues relating to vulnerable adults. Autism is a notable exclusion; there are other categories as well.

We come to the problem mentioned by Lord Lipsey, which is that either you have to engage with content to block it or you might not be in a

place to recognise the harmful nature of the content. This is particularly so with content on, say, self-harm, where part of it is legitimate cries for help and being part of a community. That is quite a difficult problem anyway.

The question is: what sorts of tool will be built? The amendment is not very detailed. We have the words “effective” and “proportionate”, by reference to size as well as the risk of harm. As I said, how well do we know what the nature of the problem is? How will we assess effectiveness? We will get no information to start thinking about where the improvement could lie. Maybe Ofcom can do some work on that, but we need to look at what its risk assessment and risk profile duties are to work on what “good” looks like.

We need to be a little more inventive in looking at tools other than filters and blocking. I am not a technologist, but we might need to have some more open-ended discussions about what sort of tools could work if we are putting all the responsibility on to vulnerable people, which is what these amendments do. We need better tools.

Dr Edina Harbinja: I am concerned that it would be difficult, if not impossible, for platforms and small and medium-sized businesses to identify the particular context of eating disorders or adults with learning disabilities because of the complexities in identifying those groups and empowering them, especially if you are using algorithms. How can you ever account for that and identify who these individuals are?

Similarly, the problem of age assurance and identifying children is impossible. You will never be able to identify children in all cases. They will always be able to circumvent some of the age assurance technologies.

Thinking about the balance between age assurance and data protection and privacy is something which the committee can perhaps unpick a bit further, with experts on the economy and technology of age assurance.

Some of these protection issues—such as the tools and empowerment—cannot be solved by asking platforms to solve them. Those issues need to be solved through media literacy, investing in social care, investing further in education, and empowering children to get to a level of understanding of the implications of the technologies they use and claim to understand. Obviously, with the effects of the harms on them, they do not adequately interact with those technologies in all cases. Very sad and tragic cases happen, as we know.

Professor Lorna Woods: I do not think we need to set the threshold for success at 100%. I do not think any legal regime—certainly any regulatory regime—achieves that. I think 80:20 would be a huge success. The threshold for success is lower than 100%. It is very easy to say that the Bill will not work in all circumstances, but that is not a justification for doing nothing or saying that this is about media literacy or society. We need to look at those areas as well, but there is a mix of elements that need to come in.

Baroness Bull: I can understand the importance of media literacy,

learning and so on for children. However, you seemed to say that for somebody with a severe learning disability, for instance, the only option is social care, by which you mean a person sitting by who is monitoring and guiding them, which has quite an interesting impact on privacy and freedom, and indeed on resources. That is a bit of a bleak outcome.

Q8 The Chair: We will not get into a lengthy debate about this. I will ask Mr Collard a question, so if he wants to pick up something in relation to what we have just heard in the course of answering that, I am happy for him to do so.

On the question of age assurance, why has the NSPCC not decided to campaign for legal age limits for platforms or for the use of social media generally? Was that considered and rejected? If so, why? This seems to be gaining momentum now.

Richard Collard: It is an interesting point. We would go back to the fact that children have a right to go on the internet and use a range of sites, because it is a way for them to learn, socialise and play. Ultimately, we need to make sure that the content they receive is age appropriate and does not put them at risk.

It would be really hard to say that there is an age you have to be for gaming platforms, for instance, because some games completely differ—for example, a LEGO game versus “Call of Duty”, where you are running around with a gun. Different age limits may be appropriate, so I do not think it is right for the NSPCC to try to say at what age a child should go on to a particular platform.

The principle of making sure that children are safe from harm is where we need to focus our time. Ultimately, the multitude of platforms that are out there have the best understanding, first, of their user base; and, secondly, of the content that is available on their sites and how they enable children or other users to see or experience that content. We would try to stay with that principle, rather than calling for specific age ranges, and, obviously, to make sure that companies or platforms are enforcing an age limit where they have one. We think that is appropriate. They should not allow children on to porn sites, for instance.

I want to quickly pick up on the media literacy point. Obviously, we agree that media literacy has a real role to play, but we cannot rely just on children to defend themselves against a range of harm in their experience online, whether it comes from grooming or the algorithmic amplification of harm. For example, a child who experiences pro-anorexia content often does not understand why they are viewing it, but a design decision in the platform has algorithmically amplified that piece of content to that user. Just teaching children not to engage with that type of content will not be the only way to solve this. We need to make sure that these platforms are safe by design.

Q9 Lord Vaizey of Didcot: This has been a very interesting discussion, although I sympathise with what Julian Knight said in the debate yesterday about just passing the Bill and getting on with it. I think this is

the end of the beginning; we have to get some regulation going.

I hesitate to ask whether there are any other issues that you want to cover that have not been covered in the Bill. Some of the points that have arisen in relation to things that you have been involved with, particularly for Professor Woods and Dr Harbinja, are about the balance of power. Has the Secretary of State, who has power over Ofcom anyway, got too much power over Ofcom in the Bill?

Dr Harbinja talked about the idea that there is too much focus on content in the Bill and not enough on processes and systems, because this is all coming out in the code, which Ofcom is yet to publish. When the Bill comes to us, should we look at getting the Government to be clearer on what the systems and processes may be, and on the Secretary of State's powers?

Matthew talked about encryption. I would love to hear whether there is anything on encryption that is not covered in the Bill that we should return to. I do worry about the ability to survey encrypted messages. Richard mentioned young people user advocates. If there are any other issues that you want to cover on the NSPCC, please go ahead. Obviously, you have complete freedom to be as brief as you want to be.

Dr Edina Harbinja: Thank you for those questions. I agree that the Secretary of State's powers are too broad and overarching. They have improved slightly with some of the parliamentary scrutiny and the negative and positive resolution processes for some of the measures. However, I am still concerned for example, about the Secretary of State having the power to determine category 1 service providers and their thresholds and the priorities for Ofcom, as well as some of the codes of conduct that they have to approve which fall under the negative resolution process in Parliament. I am concerned that these issues are still not resolved.

I am also concerned about the area of legal certainty and legitimacy, with issues such as the protection of privacy, freedom of expression and codes of conduct. I think the duty in the Bill to have regard to freedom of expression and privacy is now in Clause—

Lord Vaizey of Didcot: Do not worry about the clause.

Dr Edina Harbinja: I do not think that having the duty developed by Ofcom and approved by the Secretary of State meets the threshold for legal certainty prescribed by the law in terms of the European Court of Human Rights. I think systems and processes came under Professor Woods' comment.

Lord Vaizey of Didcot: Apparently it was you.

Dr Edina Harbinja: On the question about systems, I did say that the Bill is heavily focused on content. When it comes to systems and processes, there are provisions about terms of service and different measures, including algorithms, and the systems and processes to deal with illegal and priority illegal content, et cetera.

To respond to your initial comment on needing to pass the Bill, I respectfully very much disagree.

Lord Vaizey of Didcot: I was not expecting that.

Dr Edina Harbinja: In terms of passing the Bill just for the sake of regulating platforms and the internet, we have quite a lot of regulation, and a lot of the media forgets about that. The regulation of the internet exists in many areas.

Lord Vaizey of Didcot: Given that we have a Bill, I am interested in whether you think there are other things that could be in it, but I take your point about no Bill being better than this Bill.

Professor Lorna Woods: I have a lot of problems with the Secretary of State's powers. I have a couple of small papers and blogs about it. I divided them into two categories, broadly speaking. The first category is those that related to the scope of the Bill—the categorisation and the priority harms. I was not wildly happy about those, but there has been improvement in moving to positive resolution for some of the priority harms. I still think that for children we should have a list and a schedule with the priority harms and the primary priority harms in there, and we should be able to see that. That would stop more delay, because there will be a long delay when this comes into being, so that takes one off the list for Ofcom.

The other category is implementation, which is where the heartland of independence has always lain. It is entirely right for Parliament—and I mean Parliament, not the Executive—to set the overarching goals for a regime, but how it is implemented is for the independent regulator. We have a number of provisions where the Government can interfere. With regard to the exercise of powers, they can give guidance. Then, as Edina mentioned, there are the codes.

Lord Vaizey of Didcot: I think you are concerned that misinformation and disinformation are not covered in the Bill. Short answer.

Professor Lorna Woods: Yes. I would add violence against women and girls. I note that the commissioners will be added, but it would be helpful, given the nature of the problem—I will use the word “systemic” again, because it is not just about a series of individual instances but about how things fit together—a code would help to draw that through. There are some quite distinctive problems of violence against women and girls, which I will not go into here.

Lord Vaizey of Didcot: I think we will move on now.

Professor Lorna Woods: May I say one more thing? You might want to look at the list for user-empowerment tools anyway, because it is narrower than the Written Ministerial Statement earlier in the summer.

Matthew Feeney: We spent a lot of the first part of this session talking about content that is harmful to children. A lot of people might be concerned when looking at the Bill that what “primary content that is harmful for children” means is up to the Secretary of State.

That leads me on to one of my criticisms of the Bill, which is that it bites off much more than it can chew. Ideally, it would be split into designated Bills—one for child safety, one for fraudulent advertising, and one for criminal speech—so that the nuances of content harmful to children could be listed in a specific way.

On encryption, I think the answer is that there should be an explicit prohibition on the Government mandating the monitoring or reading of private messages. If someone wants to build a system like WhatsApp or Signal where messages are encrypted by design, that needs to be protected in the Bill.

Something that has not been discussed, and I am happy to refer Members to relevant literature, is the anti-competitive effects of the Bill. Powerful market incumbents will be best placed to comply, given their army of lawyers and engineers. I would like the UK to have a vibrant, innovative and competitive tech industry, and I worry that the Bill will entrench market incumbents.

Lord Vaizey of Didcot: That is a very good point.

Richard Collard: I have two main points. First, we completely agree with Lorna that we need to make sure that violence against women and girls is recognised in the Bill. Girls face—oh, you want me to move on?

Secondly, I want to challenge the point on privacy and end-to-end encryption being exempt from the scope of the Bill. We know that private messaging is at the forefront and the front line of the child-abuse battle. Some 94% of approaches to children by someone they do not know first take place on private messaging. We need to make sure that the Bill is technologically neutral and we do not exempt any particular technology from it.

We know that if end-to-end encryption is exempt from the Bill, that will create two incentives. The first will be on platforms to implement end-to-end encryption on all their messaging as a way of exempting themselves from regulatory obligations. A platform that previously had no intention of end-to-end encrypting its private messaging could do that and then would not have to search for child abuse, child abuse images or grooming. That is really concerning.

We know that this does not have to be a binary choice. There is a third way between both privacy and safety. For instance, Professor Hany Farid, who invented PhotoDNA, which is the main tool for hashing abuse images, said that scanning is possible in end-to-end encrypted environments without damaging privacy. It just requires companies to commit to engineering resource. We also know that Meta is investing in how to run targeted adverts in end-to-end encrypted private messages, because it has a financial incentive to invest in that. If the Bill is technologically neutral, there will be an incentive on platforms to develop technology that preserves both privacy and safety.

Lord Vaizey of Didcot: Thank you very much. I think that debate on encryption segues neatly into our final question.

The Chair: It might not necessarily be the final question.

Q10 Lord Foster of Bath: This is an opportunity to carry on the debate that we have just been having. You are well aware that a large number of amendments will be tabled to the Bill in the House of Lords—the Government have already told us about some of them—regarding communication that encourages self-harm, the sharing of intimate images, and violence against women and girls. You have variously talked about some that you want to see: user advocacy arrangements, the publishing of risk assessment, and naming a responsible individual. We have already had discussions about the powers of the Secretary of State, child exploitation material and—one that I think is very important—issues of journalistic content.

I ask you to help us, with all your expertise, on which subjects, of all the subjects you think will be raised, will be the most significant—the ones that, if we are ultimately going to get on with it, we should focus on with detailed scrutiny.

Richard Collard: I will talk through, at a high level, the types of amendments that we are expecting. Please ask if you want any further details. In making sure that the Bill prevents child sex abuse and harm to children and is implementable, the two amendments that we think are most essential—we have been arguing this for a while now—are user advocacy arrangements for children and named-manager responsibility and accountability. Both were taken to a vote in the Commons last night and they share cross-party support at the moment. We think there is already clear support in the Lords for these two and that we could get them through. We also think that, in order to mitigate some of the implications of removing “legal but harmful” to adults, there need to be minimum standards on age assurance, set by Ofcom, and the removal of the child-access assessment.

There are two other amendments that are very important for ensuring transparency in the regime. One is making sure that researchers and civil society can get access to data from the technology companies. We know that at the moment those companies are very restrictive about the data they have; they provide preferential access to data only to researchers who are basically on their side and paid for by them. If we are really to understand the impact of regulation as a whole and of these technology companies, we need to be able to shine the light on them through transparency regimes.

Lord Foster of Bath: Could I stop you there? I am asking you not to respond to this now but to write to us. You are well aware of the discussion currently going on about data mining. Under the IPO’s rules, that data would become more freely available, and a lot of people are very concerned about that. I would be very interested in the NSPCC’s views on that. Please carry on with your list.

Richard Collard: Sure. The next one is ensuring that bereaved parents can have access to data where there is a reasonable belief that the platform contributed to the death of a child. There is a group of bereaved

parents campaigning for that at the moment. We think that is a really noble cause and we fully support it.

There are two more areas that we think the committee should pay close attention to. We expect that some organisations and people will attempt to further dilute the child safety duties and try to exempt end-to-end encryption from the scope of the Bill. For all the reasons I have given today, we think that should be heavily pushed back against.

Lord Foster of Bath: Again, it would be very helpful to hear from you on this issue, although not now. Currently, there is a lot of debate about coroners' responsibilities in determining cause of death in the case of suicide. I am slightly surprised that you are suggesting that it should be the parents rather than the coroner who have access to the data. Again, please write on that.

Matthew Feeney: As I mentioned earlier, ideally the Bill would be split into other Bills and debated separately. I am not optimistic that that will happen.

Given the Bill that we have, what amendments should be priorities? One is what we discussed earlier: the Secretary of State's powers need to be scrutinised.

I respectfully disagree with Mr Collard about end-to-end encryption. I am happy to write to you with my thoughts on that in further detail.

I think that, as written, the Bill is potentially a threat to the security and privacy of millions of law-abiding British citizens, which is a concern.

I would also like to see some regulatory guidance on the actual storing of information once age has been assured in some way. The idea of a database full of personal identifiable information of people is very attractive to criminals and foreign adversaries.

Lord Foster of Bath: That problem was already solved about five years ago by the BBFC with its age assurance proposals. If you do not agree that it has solved it, let us know, but there are solutions there.

Professor Lorna Woods: I agree with Mr Feeney about the Secretary of State's powers. I think there is cross-party support for changes there, with a particular focus, as I have said, on Ofcom running the regime rather than setting the strategic objective. As I have said, I would like to see a requirement on Ofcom to have a code on VAWG—violence against women and girls—because of the need to join it all together.

We have questions about what has happened to advertising in general. It now seems that the content of advertising is completely outside the regime, with the exception of fraudulent advertising, so a bad actor could use the targeted advertising regime to get around restrictions on content. There are some quite serious bits of content that have not been thought about. What happens to extremism, content that falls short of the criminal threshold—there were, I think, questions on that in the debate in the House yesterday—and the radicalisation problem?

As I have said, and I think I am agreeing here with both Mr Collard and Mr Feeney, there is an issue about priority “harmful to children” content and primary “harmful to children” content. We should see a list in the Bill.

Dr Edina Harbinja: I agree with Mr Feeney that ideally this Bill would be split into a number of specific Bills, but I am also aware that this is quite idealistic on my part.

To be a bit more realistic, I agree, again, with Mr Feeney’s comment about new Clause 106, on encryption, and that greater scrutiny is needed when it comes to mandating accredited technology to monitor private communications. A work by Professor Ross Anderson has a counterargument to that of a work by the academic who Mr Collard mentioned: that it is impossible to do this and to have client-side scanning that does not compromise privacy.

I am also concerned about Clause 120 on the proactive technology mandate. That also threatens to introduce general obligations on the monitoring of communications and content, and again impacts user privacy.

I am really concerned about Clause 166, which I mentioned earlier, on service providers judging illegal content. This is my realistic amendment: that the standard “reasonable grounds to infer” is changed to “manifest illegality” as the established legal standard in that clause and Ofcom’s duties in Clause 167 on guiding service providers as to how this can happen.

Finally, again, this is probably not realistic, but new Clauses 15 to 17 break down further content of broadly democratic importance into journalistic content, content of democratic importance and news publisher content. Those are very different categories with different duties and different complaint mechanisms, expedited and non-expedited. I have written and argued on this, and I can write more about it, if you would like.

Lord Foster of Bath: That would be very helpful.

Dr Edina Harbinja: This is a very overlapping area, where political speech could fall within all three categories, yet the consequences are very different. So I am concerned about those too.

Lord Hall of Birkenhead: I would love to hear more on that, if we could.

Lord Foster of Bath: Absolutely.

The Chair: As much Lord Foster is keen to hear it, I am sure that Dan, the clerk, will be in touch afterwards to ensure that it is available to the whole committee.

Lord Foster of Bath: Professor Woods, you talked about an issue with advertising. I assume that you are talking, in effect, about direct marketing, as opposed to widescale advertising, or were you actually talking about more general open advertising?

Professor Lorna Woods: I was talking about targeted advertising.

Lord Foster of Bath: So what we would see as direct marketing.

- Q11 **The Chair:** Professor Woods, bearing in mind what you said at the start of the session, if witnesses are acknowledging things that are realistic versus things that are idealistic, do I take it that the Carnegie UK Trust, albeit that it was supportive of the earlier version of the Bill, is likely to campaign to reintroduce the previous version of “legal but harmful”, or do you now accept that that has gone and you accept the Government’s changes? I am keen to know whether you consider it a debate that continues.

Professor Lorna Woods: I am not sure we have come to a conclusion on that. In particular, I have concerns about the loss of the risk assessment. That is fundamental, and we will certainly express our views on that, perhaps in more detail. Linked to that is the obligation to summarise, which is now being brought in for children and for harmful content.

For Carnegie, the risk assessment, which is the bit of the Bill that focuses most clearly on the features, functions and characteristics rather than on content, is the important bit for understanding information flows and trying to move away from just saying, “Let’s take stuff down”. That is particularly valuable where you are talking about content that is not contrary to the criminal law but that may have some sort of intersection with regulatory law or private law or be otherwise harmful.

I am not sure about fighting for Clause 13, as was, but I would certainly emphasise the risk assessment—Clause 12, as was.

- Q12 **The Chair:** Finally, Mr Feeney, I thought at one point that the situation might now have moved from a battle between freedom of speech and child protection to one between privacy and child protection. Do you feel that the battleground of freedom of speech has shifted, or is it still live? I would like your general view on that.

Matthew Feeney: I still think that the issue of free speech is very live. I published a paper, before the most recent amendments, arguing that the biggest threats posed by the Bill were to privacy, free speech and competition. I still think that those are the three biggest threats. Obviously, the repeal of “legal but harmful” for adults is a welcome step in the right direction, but, as we all discussed earlier, as long as the child protection obligations remain, there is still a threat there.

The Chair: I feel it is only fair to ask you, Dr Harbinja and Mr Collard, whether, before I close the session, there is any final point that you would like to make that you have not had an opportunity to make. There is no need to repeat anything you have already said.

Richard Collard: No.

Dr Edina Harbinja: Yes. I disagree that the dichotomy between child protection and privacy or freedom of expression is as clear as you may have presented it and that the battleground is very separate. There are

also quite a few nuances when it comes to children's human rights to freedom of expression and privacy and to receiving and imparting information that come into play and develop as a result. I do not think it is one or the other. There are other areas, as we have discussed, but taking into account children's human rights as well is important.

The Chair: Thank you, all four of you, for your time this afternoon and for giving your evidence, which was very helpful.