

Communications and Digital Committee

Corrected oral evidence: Ofcom leadership

Tuesday 14 October 2025

2.30 pm

[Watch the meeting](#)

Members present: Baroness Keeley (The Chair); Viscount Colville of Culross; Baroness Elliott of Whitburn Bay; Baroness Fleet; Baroness Healy of Primrose Hill; Lord Holmes of Richmond; Lord Knight of Weymouth; The Lord Bishop of Leeds; Lord McNally; Baroness Owen of Alderley Edge.

Evidence Session No. 1

Heard in Public

Questions 1 – 38

Witnesses

I: Dame Melanie Dawes DCB, Chief Executive Officer, Ofcom; Mark Bunting, Director for Online Safety Strategy Delivery, Ofcom.

USE OF THE TRANSCRIPT

This is a corrected transcript of evidence taken in public and webcast on [parliamentlive.tv](#).

Examination of witnesses

Dame Melanie Dawes and Mark Bunting.

Q1 **The Chair:** Good afternoon and welcome to this meeting of the Communications and Digital Committee. We are very pleased to have with us Dame Melanie Dawes, Ofcom's chief executive, and Mark Bunting, Ofcom's director for online safety strategy delivery.

This committee has a role in scrutinising many different aspects of Ofcom's work but, today, we will focus in particular on online safety and media literacy, on which we produced a report following our recent inquiry. This session follows up on that inquiry into media literacy, which we conducted in the first half of this year, and the sessions that we held in September regarding Ofcom's current consultation on additional safety measures.

This session is being broadcast live and a transcript will be taken. Our

witnesses will have an opportunity to make corrections to that transcript where necessary. I have mentioned to our witnesses that it is possible we might have to stop for a vote in the next hour. Let me start with the first question to open the discussion.

Ofcom has described 2025 as its “year of action” for online safety. Broadly, how confident are you that the new duties on platforms are having a tangible impact on the online experiences of UK citizens? In your reply, you may want to highlight your confirmation of the £20,000 fine on the online message board 4chan, which we read about today, for failing to respond to legally binding information requests that you made about compliance with the Online Safety Act. It has been reported that 4chan’s lawyer said, “We’ll see them in court”, and said that 4chan will pay the fine, “When pigs fly”. That is not the response that we want to see from platforms. Can you talk to us about the impact you may have with such action? If you get that sort of response from platforms, what further action can you take?

Dame Melanie Dawes: Thank you for inviting us today. There are two questions; let me start with the first, then we can come on to the second.

The first question is: how confident are we that we are having an impact for UK citizens? We are very confident that we are now beginning to see an impact. Is it enough? Not yet—it is still very early days—but we are seeing an impact, particularly where age-verification rules are required across pornography and on some other platforms such as X, Discord, Reddit and Bluesky. Those age checks are very new; they came into place at the end of July, in accordance with our deadlines, but they are beginning to offer significant protections, particularly for children.

We are also seeing change elsewhere. We are beginning to see some big social media companies changing the way in which their algorithms work and the way in which they feed content to young people. We are also beginning to see changes in privacy settings to protect children from grooming, and so on. So I am confident that we are seeing change. I do not want to overplay it because there is a lot more to do. There will be some areas where we come up against more resistance—there is no question about that. I am sure that you will want to come back on many of these issues.

On your second question, which was specifically about our announcement yesterday on our enforcement cases, we have announced a number of updates. You are right that one of those was that we are fining 4chan £20,000. We also announced that a number of other small but risky companies have come into line with our measures as a result of our enforcement action. In the case of some small file-sharing platforms, that includes putting hash-matching technology in place; that is the industry standard for detecting child sexual abuse material, so that is progress.

We are seeing some companies choosing not to comply with the Act; they geo-block the UK so that their service is no longer easily available,

which offers another significant protection. There will be some that choose to ignore our enforcement action. We are going to have to see where we end up with 4chan. I cannot say much more about it today because it is a live investigation; we are also subject to legal action in the United States, as you may be aware.

Q2 The Chair: I also have a question relating to the aftermath of the horrific attack on the Heaton Park synagogue on 2 October. Many prominent Jews posted expressions of grief and sadness on that occasion—absolutely rightly so. They encountered replies full of appalling antisemitism, glorification of violence and further threats; those have been reported to us and measured.

Can you tell us how, in your enforcement of the Online Safety Act, you are requiring platforms—X, or Twitter, seems to be the one where most of this has happened—to have systems in place specifically to address these calls for violence? It is appalling, when we have an event of such magnitude and seriousness, that that is the response we see on social media.

Dame Melanie Dawes: You are right. It was a horrific act and an incredibly sad day. On some platforms, we have seen some illegal content; that is the relevant test now that the duties are in force. We have followed up with all of the big companies to find out what they have been doing. Our experience last summer, during the Southport riots, was that, where companies had emergency protocols in place, they made a really big difference; their systems were the first to say, “OK, we have a crisis. We are going to stand up a response”.

Secondly, those systems went through all of the things you would expect, such as considering whether there was a risk—for example, with videos of the attack, which can be really harmful—or whether there was a risk of incitement to violence, and so on. Companies that had those protocols in place did a better job of managing and mitigating the risk of illegal activity on their sites last year. So, in our additional safety measures consultation, we have set out that large sites need to have those protocols in place because our evidence suggests that they do make a difference.

We are going to find out whether, in the past few weeks, the protocols that were stood up made a big difference to whether some of the risks could be managed.

Q3 The Chair: What action can you take? I specifically mentioned X—Twitter—because that was raised with me as one of the sites where most of this was happening. What specifically can be done?

Dame Melanie Dawes: The test of the Act is: do they have systems and processes in place? Are they moderating their content adequately? When they find illegal content, are they taking it down?

The Chair: If there is a peak like this, clearly, they are not.

Dame Melanie Dawes: Exactly—that is the conversation we are having with a number of companies, using the events of the past few weeks to crystallise whether their measures are working. I cannot say more at this stage about where we are with particular companies, but it is an active conversation. We reached out to all the big companies that day to find out what they were doing; we will follow that through.

Q4 **The Chair:** Can you say anything else about how you are measuring the impact of the Act—on using information-gathering powers, for instance?

Dame Melanie Dawes: It is in two parts. First, we will investigate whether companies are putting in place measures such as age assurance, changing the way algorithms work, content moderation, grooming protections, et cetera. That is quite tangible. The public like to have the dialogue in those terms; it is more relatable to their experience online, so it is a really important part of the picture. In our annual report this December, we will publish our first assessment of what is going on and who is doing what. In our letter to you, we talked about some of what is going on with age assurance; we can expand on that today if that would be helpful.

What is happening on platforms online is a really important part of the picture. Where we need to use our information powers, we will. If we need to do something systematic, for example, it can be a very effective tool for us, but we do not always need to do that if we have already had it disclosed to us or it is publicly known.

The second part of this is probably what matters the most: are adults and children experiencing a better life online? What we are doing there is a whole mix of different bits of research and evidence-gathering, recognising that this is not a question that the industry has asked itself in the past; it is new. We have a long-standing panel survey of children's and adults' experiences online, which we expanded a few years ago to be ready for this. There is fieldwork going on this autumn, which will be the first time when we get to see whether the changes that have come through in the summer are starting to provide a different experience for children and adults; that will be published next May.

Mark Bunting: May I build on that momentarily? I want to pick up the point that Melanie made about the industry having not gripped this issue. This work—particularly in gathering data from firms about the experiences of users on their platform—is, as far as we know, new for a regulator in this area anywhere in the world. There is currently no industry standard for what safety looks like online. So the first step for us will be to set out the measures that are available to companies and how we should understand the data that is coming out of firms. As Melanie says, we will publish that over the next few months. It will take some time to get to a point where the industry is consistently applying the measures that are needed to track progress, but, again, as Melanie said, creating a safer life online is the core of the job that Parliament has set us. We will be looking to make that a priority for our engagement with industry over the coming years.

Q5 **Viscount Colville of Culross:** Good afternoon and thanks for coming. I want to ask initially about concerns over freedom of expression. There have been concerns that the Online Safety Act and your guidance mean that some platforms are adopting a bypass strategy; and that their moderation is much broader than it needs to be because they are worried about judgments on illegal content. Do you recognise that concern? Do you think that you can do anything to ensure that companies do not moderate quite so broadly and, therefore, do not restrict freedom of speech?

Dame Melanie Dawes: I definitely recognise the concern around freedom of expression; it is on the front page of the Act that it needs to be respected. We need to make sure that what we do as a regulator does not restrict it in a way that is not required by the Act.

It is not the case that our guidance or codes are encouraging what we might call overmoderation. We have seen, particularly over the summer, that, as the age restrictions came into place, some platforms chose to treat users whose age was unclear as children for a few weeks while they gathered the data that they needed to confirm that they were adults. Those users found that they could not access some content that would have been fine for adults but not for children; there was some of that going on.

Also, it is the case that some platforms choose to have content standards—they are usually called community guidelines—that are about not just illegal content but, for example, restricting hate speech more broadly. That is a choice for them but it is not required by the Act; we need to be clear about that.

I do not think that that is being caused by the Act at this point, but I do not want to be complacent; it is something on which we will be keeping a very close eye. There is a risk that some companies will overmoderate because they want to make a point about the Act and to claim that it goes further than it actually does.

Q6 **Viscount Colville of Culross:** What can you do about that? Because you are required by the Act to guard freedom of expression, if you spot overmoderation, what can you actively do to ensure that it does not take place?

Mark Bunting: I want to pick up a couple of things. One point links back to the conversation we were just having about data gathering from platforms. We are looking to the big platforms to give us data about content that they have acted on wrongly for whatever reason—where they have acted on content that does not contradict our rules or their own terms of service. That will shine a light on the extent to which there is a problem.

The other thing we have done is provide very detailed guidance—mainly for firms that want only to stick to the letter of the law—on how they should identify illegal content when they come across it. If we think that there is a significant problem, that gives us a basis to talk to firms in

order to understand why their own internal guidance to their moderators might not be aligned with the guidance that we have provided.

Q7 **Viscount Colville of Culross:** That is very helpful; thank you. I want to move on to privacy. There has been lots of concern that the HEAA requirements mean that you have to give away your personal details and that those can be exposed to data breaches and the data being misused. Is there any way in which you can develop a stricter data handling requirement, or even require that those details should not be personal? There should be hash-matching and other, non-personal ways of doing age verification.

Dame Melanie Dawes: In our guidance—again, it is in line with the Act and UK law—we have said that, when companies implement highly effective age assurance, they must respect privacy and data protection rules. If we see a concern, we will report it to the ICO. That is very clear; I do not think that any company out there thinks that we are trying to fudge the privacy issue with our guidance.

We have given companies quite a lot of options, many of which do not require them to collect—certainly not to keep—personal data at all. For example, many companies, though not all, are using facial age estimation. You hold your phone up to your face and it estimates your age—quite accurately these days. Again, if you are obviously an adult, you will go straight through to that service without anything further needing to be done—no name, no address and not even what your actual age is. It is just a yes or no question: “Are you over 18?”

Likewise, companies can use data that is already available either through email verification, which is a service that some third-party suppliers provide, or by relying on the fact that they may already be using credit cards for payments. If they are, that is great because it will confirm that the user is over 18—but, again, not who they are and no details of the credit card arrangement that go beyond what has already been collected. We are very clear about this.

I am sure that we are going to find some cases where there are issues around data protection. There was one last week with Discord; it reported itself to the ICO, and the ICO will look into that. It has done the right thing. It has introduced age assurance. I am glad that, when it had a problem, it reported it quickly and went straight to the ICO. From our perspective, that means that the system is working.

Q8 **Viscount Colville of Culross:** Would it be helpful to assuage people’s concerns about privacy in this area by recommending to companies that they do not require personal details as their main standard for eliciting age; and that they should use other technologies or techniques that are available?

Dame Melanie Dawes: We have done a lot of work with the Information Commissioner’s Office on this. All of our guidance has been confirmed and approved by it as being consistent with UK law. As I say, we have been quite flexible and clear that privacy and data must be

protected, so I am not sure that we should be too prescriptive here. It is a balancing act. If you start to add further requirements, it makes the guidance harder to engage with.

One reason why we have had considerable success in getting age checks put in across the porn industry this summer—beyond what most people, including ourselves, were expecting, to be honest—is because we have not been too prescriptive. We have allowed a number of options. We are clear about the outcome, but we are not being too prescriptive about the mechanism. That is one of the reasons why they are playing ball, as well as the fact that we are enforcing against it.

Q9 **Viscount Colville of Culross:** Moving on in the privacy space, I want to look at encryption. There is a concern that the Government's demand for Apple to grant access to people's personal data threatens to weaken privacy. Section 121 of the Online Safety Act gives Ofcom the power to pursue personal encrypted data, but there is no guidance on the rights and security concerns of such a power. Are you developing guidance on how to deal with encryption, and are you trying to ensure that people are not concerned that their privacy will be invaded?

Dame Melanie Dawes: I might ask Mark to pick that up but, just to clarify and put it on the record, Ofcom has not been involved at all in any actions from the Home Office.

Mark Bunting: On encryption generally, the Act is quite limited in terms of the extent to which it bears on encrypted services; the Government and Parliament were clear during the passage of the Act that they did not think it was appropriate for the regulator to have powers to prevent companies using encryption. There are, of course, many good reasons for consumers to prefer encrypted services. For example, in the Act, we cannot require companies to use scanning tools in private communications environments to maintain that protection of privacy; that would often include encrypted environments.

On your point about Section 121, that creates a mechanism where, in very specific circumstances, we can require the use of technology that has been accredited through a process led by us to detect child sexual abuse material, including in private spaces. We are still in the early stages of that process.

We have to provide advice to the Secretary of State about the thresholds of accuracy for those minimum standards; that will then be considered by the Secretary of State and written into secondary legislation, after which we can start the process of accrediting technologies. That is the main mechanism for us. It is quite limited and, of course, it relies on technology being available that meets those standards of accuracy to detect child sexual abuse material.

Viscount Colville of Culross: But it is under way?

Mark Bunting: The work is under way, absolutely.

Dame Melanie Dawes: Can I just add something? It is not clear at this point that those technologies will be available. We will go through the process, but it is a high bar because of the concerns around freedom of expression.

Q10 **Viscount Colville of Culross:** Finally, I want to get on to the knotty issue of VPNs. In your letter, you said that one in 10 under-18s is using VPNs to get around age verification. Is there something that you can do to introduce age verification for VPNs, particularly when it comes to app stores? Should you have age verification on app stores to make sure that access to VPNs is limited for under-18s?

Dame Melanie Dawes: The data we have, which is from Internet Matters and from before the summer, is that one in 10 children is using VPNs. We are going to check that through our own research; we hope to have a better feel for it in May, with the tracker I mentioned earlier, because it is really important.

VPNs can be used to bypass the protections of the Act and very determined online users can get around the protections, if that is what they really want to do; through a VPN, they can, in effect, be in another jurisdiction or in none. The six-million-dollar question right now is: are children doing that? Are they bypassing the protections for pornography in a way that would concern us all? We take a lot of comfort from the fact that all of the research shows that most children stumble across porn unwittingly; therefore, the age protections should significantly prevent that already, but we will keep this closely under review so that we can all be sure that the protections are working as we intend.

On what one can do about VPNs, Mark may correct me but I do not think that age verification in an app store would allow an app to know that somebody is using a VPN. I am not sure that that link quite works. We are not able, for example, to put an age restriction on VPNs at the moment; that would be a policy question for the Government. To be honest, our view at Ofcom is that this is an area we all need to understand better. The spotlight has not been here before, so we are going to be contributing as much as we can with our research. If the Government do decide that they want to legislate in this area at a future date, we will have as good a grounding in it as we possibly can have.

Q11 **Viscount Colville of Culross:** Are you doing research into this?

Dame Melanie Dawes: Yes. It is into the use of VPNs by children and adults, but particularly focusing right now on children. That will cover not just whether they are using them but why and how they are using them.

Viscount Colville of Culross: There is no deadline, right? You are not waiting for the Government to come in—

Dame Melanie Dawes: No. We are doing this because we think that it is important. We have a tracker that does fieldwork twice a year and is very flexible; we can put whatever questions we want into it. We also do ad hoc work. A big part of what Ofcom does has always been to make

sure that we research users and consumers as well as we can, so we will have a much better understanding of this in six to nine months' time.

Mark Bunting: I have one more point on this, if you do not mind. The immediate media coverage when we introduced the age-checking rules in July might prove to have been a little overdramatic. We saw an increase in VPN usage immediately after 25 July, when the rules came into force, but we are already seeing signs of that tailing off. The numbers are relatively small, as compared to internet use in the UK. We saw a peak of around 1.5 million VPN users out of an online population of 70 million in the UK; that 1.5 million figure has, over time, started to come back down closer towards 1 million. So far, we think that the evidence is that VPN usage is not mainstream in the population, but, of course, we are waiting for further evidence to make sure of the evolving picture.

Viscount Colville of Culross: I do not want to accuse you of complacency, but one in 10 under-18s using VPNs sounds like quite a lot.

Dame Melanie Dawes: It depends on what age they are. The evidence suggests that it is older teenagers. In talking to children, they have said that, for example, sometimes they get a better connection with one than what is offered by their school. We just need to understand this better. If that one in 10 is all older teenagers, we would obviously be much less worried about it than we would if it were nine, 10 or 11 year-olds. We recognise that, prior to the restrictions, pornography was being found by one in 10 nine year-olds; the vast majority of children were stumbling across it for the first time without having intended to seek it out.

Q12 **The Chair:** I am getting reactions from the members, though, that that does not sound very safe. I know Jim wants to ask a follow-up question, but if it is one in 10 and 1 million, we are talking about 100,000 children.

Dame Melanie Dawes: It is 1 million overall, and one in 10 children, according to the Internet Matters research from this summer.

The Chair: How many children are we saying that is?

Dame Melanie Dawes: It is 1 million daily uses of VPNs across the whole of the population, and one in 10 children from eight to 18 years of age using a VPN from time to time. They will not be using it every day, and the numbers do not include young primary school-aged children, so it will not be as many as 1 million.

The Chair: I find that the reaction in the committee is that any level is not acceptable if it allows them to access pornography.

Q13 **Lord Knight of Weymouth:** We have noted your differentiation between older teenagers and younger children, particularly when we come later on to discuss a rigidity in the regime around age-appropriate design. You are either a child or not a child for most of the regime. So those comments are noted, and in my case they are certainly welcome.

But in respect of VPNs, we know that through access to sport, where there is a lot of money at stake in terms of sporting rights, the

technology exists to detect the use of a VPN. I assume that the geo-blocking you referred to earlier can be overcome using VPNs. So, there are different ways in which VPNs can be used to circumnavigate the regime that we have put in place.

Are there not certain types of categories of service where you should be expecting them to use the same technology that Sky and other sporting rights holders use to detect VPNs?

Dame Melanie Dawes: I do not think it is straightforward. Sky and others have a subscription service; they do not want people to be using it outside the UK because it is only supposed to operate in the UK, and they have a commercial reason for doing that. We are happy to come back on that, but my understanding is that there is not a simple way for companies to know all the time that people are trying to access their service from outside the UK, or outside a UK ISP address. Unfortunately, I do not think it is as technically straightforward as we might wish. That is my understanding based on a number of different conversations we have had over the last few weeks, but we are happy to come back on that.

Ofcom is not saying that it is not concerned that there is a risk that VPN use could undermine the protections of the Act, but we have to be realistic; VPNs are legal. They come with many advantages. A lot of companies use them to protect data when people are accessing their systems over public wifi, for example. So, they are a part of the modern internet. The question is: what other layers of protection can we put in place? What assurances do we have? The importance of parental controls is very relevant when it comes to VPN use by kids. The operating system providers, Apple and Google, are now strengthening their age protections at the operating system level and providing much more obvious and easy-to-use functionality for parents to restrict, for example, whether VPNs can be used by their child. So that is another route in for protections.

There are very few silver bullets with online safety endeavours. We have always got to be alive to the fact that something will work and will achieve an impact, but we will always need to be thinking about further layers. It cannot be about perfection; I just do not think that is realistic. But it can be about a constant endeavour to improve protections, and that is how we see it at Ofcom.

The Chair: Thanks for offering to come back to us; we would be very interested in that.

- Q14 **Baroness Owen of Alderley Edge:** The committee has heard from a number of witnesses who have criticised Ofcom's approach to implementing the online safety regime, saying it is more incremental than iterative and that it lacks a clear goal. I am going to read you the quote from the Molly Rose Foundation; one witness described it as a "gradualist approach" that "is slow and reactive". How would you respond to that?

Dame Melanie Dawes: I do not agree; I do not think it is gradual. Our illegal harms codes, children's codes, and age verification guidance all represent a step change for the industry. Yes, some of what is in the illegal harms codes in particular is already best practice and in place in some companies, but there are lots of things that we have asked for, including our grooming protections, for example, which are not at all standard across the industry, and it is a big shift, even for the biggest platforms, to be implementing those. We think the substance of our codes is a very big step forward on multiple fronts.

However, we also knew and were very open and honest about the fact that the first version of the codes was only ever going to be that. We produced the illegal harms codes for consultation less than two weeks after the Bill became an Act; we knew we were going to have to follow it up, and we got lots of ideas from civil society—including the Molly Rose Foundation, in fact—that we have put into our quite quick additional measures consultation, which is still running now but contains a number of additional protections. We will continue to have this bank-and-build approach, which is to keep enforcing against what is already there but building and adding measures if, for example—as Lord Knight and I were just discussing—we need to put more protections in because some that we put in first were not as effective as we would all want.

- Q15 **Baroness Owen of Alderley Edge:** Do you believe that this approach will allow Ofcom to keep pace with the latest developments in online harms and technologies? I give the example of AI chatbots, which have recently featured a lot in the news; there have been some horrific cases both here and in the United States on children's interactions, and there are further issues around interactions between adults and AI chatbots.

Dame Melanie Dawes: This is a challenge for any legislation when the landscape is moving so fast. The good thing about the Online Safety Act is that it is technology-neutral. What that means is that, in quite a lot of places, companies that we are already regulating are introducing, for example, new chatbots, and they are caught by the Act because it does not matter whether those chatbots are run by technology or by a human being. So the flexibility of the Act is helpful in this respect. But will it capture everything we are worried about? For example, will it pick up every self-standing chatbot, which is not a user-to-user service under the Act? There will be some services that are not caught in the way that we would want, but there are many that are caught. So, for example, we are regulating ChatGPT as a search service because we believe it falls within the scope of the Act. It is inevitable that you can never account for everything, and if you try to be too prescriptive, then you are not able to cope with change. In some places the Act will be able to deal with this and in others it will not, and we will be keeping a really close eye on that and engaging with the Government in case they want to bring forward any changes.

- Q16 **Baroness Owen of Alderley Edge:** Do you believe that the approach is sustainable and agile enough in the long term to undertake the horizon

scanning that it needs and to adapt to that?

Dame Melanie Dawes: I would be very surprised if Parliament did not want to come back to some amendments to the Act at some point, because I do not think it is possible to legislate in 2023 and have that be perfect for ever, or even for 10 years, particularly where so much change is being driven by technology. But, as the regulator, we will do everything we can to apply our resource and in particular our enforcement efforts to new risks and new services as well as old, if that is where we think the harm is being caused for consumers. If we think that we cannot act because things are not in scope or we do not have the tools, then we will be flagging that with the Government so that if they want to bring forward a package of change, they can do so with all the benefit of our findings as well as whatever else they may wish to prioritise in terms of policy.

Q17 Lord Knight of Weymouth: I will just follow up on that while I have the conch. When the Bill was going through, you published the draft roadmap of how you were going to sequence things. It would be really helpful if you were able to write back to us and show us any changes to that roadmap that have happened in the meantime and your progress against it, so that we can see your sense of priority and urgency. We hear a lot of criticism about the right sense of urgency, and that would give us some evidence.

Dame Melanie Dawes: We are very happy to do that. In fact, we are planning to publish an update in the next month or so, and we have updated the initial one that we set out in 2023, I think, several times since.

Just generally, on this whole question of urgency, there is an awful lot of this Act to implement. There are quite a lot of things that we have not got round to yet because we had to prioritise the codes to get them in and start enforcing against them. I would like to get the point across that this is a multi-annual programme of work, even in the early years of implementation, because there is an awful lot we need to do to get it moving. We chose to prioritise enforcement and compliance in 2025 and that was the right decision. I hope you would agree. But we will publish a new roadmap so that you can see what is happening and when.

Q18 Lord Knight of Weymouth: My substantive question is around the additional safety measures on which you have consulted and are still consulting. From my point of view I welcome that, and the committee generally welcomes what you are trying to do around further processes to stop illegal content going viral, further protections for children, and tackling harms at source.

But the approach remains relatively prescriptive and, allegedly, overly focused on process rather than outcomes. It goes to this safe harbour criticism—that if they follow all the processes that you have recommended, then you are not going to take action against them even if the outcomes do not turn out to be what we want. Can you talk us

through why you have taken that approach, and how you currently view the safe harbour criticism?

Dame Melanie Dawes: We have taken that approach because it is set out in the Act. The safe harbour principle is there, and so is the requirement that the measures in our codes are clear and detailed. That is the language of the Act. The fundamental duty on platforms is to have systems and processes in place to mitigate and manage the harms that the Act sets out. So, the Government and Parliament made a fundamental choice to have the safe harbour principle and to require our codes to be specific.

If we get into the place that you are describing, where there are evident risks that are not addressed by the measures in our codes, then it is on us to try to come up with new measures. Sometimes there will be no measures; there are some areas of the Act—for example in relation to our ability to require actions in private messaging services—where there are risks but Parliament has taken a view, particularly because of freedom of expression concerns, that the regulation should not overreach into those environments. So, sometimes there will be risks that remain.

It is important that Ofcom is as transparent as it can be about where those issues remain, why, and what it has done about them, but this is quite dynamic from our perspective. So, if we saw that there was a risk assessment that was not being addressed, we would be worried about that and would try to do something about it, just as if we see a risk assessment that is not good enough—and we have seen a few of those—we would send it back and ask for a new one. We have done that a couple of times with some of the biggest companies.

Q19 Lord Knight of Weymouth: Does that transparency extend to areas where you might think that Parliament should amend the Act? I have the beginnings of a list: whether we should say that VPNs should be regulated; some issues around AI; relationship apps are a concern, and whether they should be in scope. Will you publish publicly any recommendations that you make to the Secretary of State around improvements to the regime?

Dame Melanie Dawes: We are quite reluctant to do that, especially right now, partly because it is beyond our brief. It is for the Government and Parliament to decide what future changes are made to the legislation, if any, and it is our job to get on with implementing what you have already given us.

We have a lot to be getting on with, and I go back to Baroness Owen's question earlier: what is in our codes is very significant and is already starting to drive important change that is going to improve things. We need the industry to focus on that and get on with it and not to use any future legislation as a potential distraction from the job in hand.

Q20 Lord Knight of Weymouth: On my part, I agree that we are making some improvement, and I am proud of the legislation that we took through.

You are proposing using proactive technology measures to help in terms of these additional safety duties. In what ways do they go beyond existing industry practice? Is there anything really new there?

Mark Bunting: These are going to be really important measures. It is true that some of the bigger companies in particular use proactive tech tools, as they are called. What we are really talking about here, as the committee will probably be aware, are tools that allow for the automated scanning of large quantities of content so that services can identify illegal content before it is uploaded and therefore prevent people seeing it rather than having to report on it afterwards. These tools are already in use, but we do not have very much information about how accurate and effective they are, and that creates two risks.

First, it creates a risk that companies say they are doing the right thing, but in actual fact the technology is not up to the job. The second risk links back to Viscount Colville's point that these things could be gathering a whole load of legitimate content and taking it down, and nobody is any the wiser because the use of the tool is not transparent. So we are trying to shine a light on that.

The second thing that we are trying to do is to encourage firms that do not use these tools currently but could do to make sure they carefully consider the scope for using these tools. Under our code proposals, they have to carry out an assessment of the accuracy and effectiveness of the available technology—not just the technology they have in-house now, but technology they could develop or buy in from third parties. If they deem that technology to be accurate and effective, and we are able to scrutinise those assessments, then they should use that technology.

As Melanie said earlier, these proposals are still going through consultation, but our expectation is that this will drive not only wider use but better use of these tools so that we have more confidence in the way that companies go about their use.

Q21 Lord Knight of Weymouth: Finally, you mentioned earlier on that the Secretary of State will set the threshold around the accuracy of these tools. Is that right? What is the sequence? You are consulting right now and encouraging people to look at them; the Secretary of State will, through regulation, publish thresholds of accuracy, and then effectively you have a standard that they will abide by. Is that roughly how it works?

Dame Melanie Dawes: There are two different sets of tools, actually.

Mark Bunting: Yes, there are two different parallel processes. We have to accredit technology in the very specific case of detecting child sex abuse material and terrorist content. We can then require a firm to use that particular technology where it has met minimum standards of accuracy.

We are proposing a different and slightly lower bar for companies to consider for themselves the scope for using these tools across a wider range of harms. That would include, for example, suicide content, self-

harm content, eating disorder content, and fraudulent content. We think it is right that firms have to take responsibility for making the judgment themselves about whether the tool is sufficiently accurate and effective for their use. That is their judgment, and they should use it; we are expecting that to drive wider use than the regulator just issuing directions.

Dame Melanie Dawes: If I could just add, it is quite a big step for us to be recommending the use of proactive technology, and we have given a lot of thought to the freedom of expression implications of this, which is why we have not proposed it for all types of content at this point. We are still open for consultation because it is a big deal. It is also a very good example of where technology is helping us. The new tools, particularly using large language models, increasingly mean that this detection or moderation is effective. It is an example of where we have responded to that. These tools would not have been something that we would have had over the bar a couple of years ago in terms of showing that they are effective and proportionate.

Q22 Baroness Fleet: Thank you so much. You have been very helpful. The Molly Rose Foundation has already been mentioned once, and you will know even better than us how hard it campaigns and how concerned it still is about the limitations of what has been done so far. Their September newsletter, which I was just reading says that “Users of Teen Accounts are still able to view content that promotes suicide, self-harm, and eating disorders, with autocomplete suggestions actively recommending search terms and accounts related to suicide, self-harm, eating disorders and illegal substances. Instagram’s algorithm incentivises children under-13 to perform risky sexualised behaviours”, and so on, and they are finding material that is accessible to young girls; they specifically mention girls because they are the Molly Rose Foundation. What is your reaction to that and how are you acting on it?

Dame Melanie Dawes: That is a really important question. First, I absolutely respect that organisations will continue to campaign and push us very hard. Although it is sometimes painful, it is what we want and need at Ofcom and I have no problem with it at all. Sometimes they are going to be getting at things that we are not aware of, so I hope that these organisations continue to bring evidence and shine a spotlight on these issues. Investigative journalism is another route that is really important, particularly at this very early stage.

They are talking about Meta’s Teen Accounts because that is one of the products that Meta has and it describes it as a teen account. What we are doing with Meta, Snap, TikTok and a number of other companies where there are a lot of children on the site—right now and over the autumn and winter—is really interrogating whether their systems work. Those systems are a combination of age checks to make sure they know how old the kids are, content moderation to classify and find the content, and changing the way the recommender systems work so that—in line with the Act—children only see a feed that is appropriate for their age.

It is actually a good example of how the Online Safety Act, and the way we are implementing it, is outcome-focused because you could put all those measures in but the only way you really know whether they are effective is by looking at the outcome. In the past, companies like Meta would have said that the prevalence of suicide and self-harm material is extremely low, at 0.0% or whatever, but we are very clear with them and others that this is not the relevant metric. The relevant metric is what happens to a 13 year-old girl when she goes on Instagram and likes various things and then gets fed all that suicide and self-harm material, which may be low in prevalence but is very toxic to that particular user. That is the test. It is a new test, not one the industry has really looked at before, and it is what we are interrogating over this winter so that we can then work out whether these concerns are a one-off but the underlying systems and processes are working well, or whether they are indicative of a wider problem.

Q23 **Baroness Fleet:** It is great that you are on it, but there is also criticism that you are too slow, and do not have enough people and skills to act fast enough to be really effective. You say “over the winter”, but you could be talking about another six months to work out what you are going to do.

Dame Melanie Dawes: Nothing is fast enough; I feel that quite often. The harm is still there, and given the nature of the harm, we cannot move quickly enough.

The children’s codes only came into force at the end of July; we required risk assessments from all the big companies by early August, just a week or so later. We have interrogated those. As I was saying earlier, we have had some extremely robust conversations with big companies whose risk assessments were not good enough. They were far too low-risk at the beginning, and we have seen some changes there. We gave them a deadline of 30 September to tell us what they are doing and how they are implementing the code measures, and now we are going to be interrogating whether they are effective. There are meetings happening this month and next month, where we are beginning to get under the skin of that with these companies. We are moving quite fast, but inevitably we have had to mobilise a lot of the regime to get to this point, so I accept that we need to keep the pace up.

Mark Bunting: Just to build on that, we set out five areas for industry at the start of the year and wrote to firms to say that these were the areas where we expected improvements. Some are fairly black and white; the use of age checks by porn firms is a good example. It is very easy to detect whether a company has done what the law says it should do. Some require much more forensic assessments and with the area you have picked up on—which I completely agree is one of the most urgent and important issues covered by the Act—we have to get to grips with how the age-check systems, content moderation systems and recommender algorithms in these companies are working together to drive experiences which are not safe enough for teenagers. We are working on that now; we have our technology teams doing algorithmic

assessments of some services. Our supervision teams are talking to firms about the steps they are taking to keep children safe. These are questions that need a lot of careful forensic investigation. It is not quite as straightforward as it is in some other areas.

Q24 Baroness Fleet: I appreciate that, but the concern is that they are always going to be one step ahead of you. You say you want something, so they start implementing it slowly, and then they think of another way of doing it and so on. It is very hard to get ahead of them and really be effective. There is real concern that they have more people and more money invested towards not being prevented from doing what they want to do.

Dame Melanie Dawes: They are always going to have more money and more people than we have. There is nothing we can do about that. What we have seen from the beginning of the year is that a lot of the social media companies have introduced changes—for example, Meta’s Teen Accounts. We have also seen changes to messaging services. Meta are announcing some further changes this morning, and we will be looking at those closely. It is an open question whether that is enough, but it is good that they have made the changes. They have made them because of regulation. They have never worked with regulators before; they are responding partly to the European Union and partly to Ofcom. But it is our job now to look at the risk assessments, make sure that they are in the right place and that they have not undercooked them, and then to make sure that the measures are in place and that they are effective. We are doing that, and we will report on it in our annual report on online safety.

In about six weeks’ time we will be publishing a separate report on risk assessments, where we will be giving a view on how this has gone so far, because we have been having a very interesting set of conversations.

Q25 Lord Holmes of Richmond: We have heard evidence that live-streaming is not safe for children, particularly those under 16. Why have you not proposed age limits for live-streaming functionalities?

Dame Melanie Dawes: That is a really important question. We are concerned that live-streaming is risky for children. We gave a lot of thought to whether we should propose a ban on live-streaming for under-18s. In the end, we have come out with a forensic understanding of how perpetrators operate around child grooming, which is the risk we are concerned about here. We have proposed some surgical measures that address what we know about perpetrator behaviour. For example, suggesting that likes for under-18s are switched off, screen capture is switched off, and payments and comments are unable to be made, as they are part of the way perpetrators groom children. That is what we have proposed. The consultation is still out there, but this is one of those areas where we have said that, if it is not enough, we will go further, because the risks are very clear.

Q26 Lord Holmes of Richmond: To develop a point that Lord Knight made

about the age of 18, you are a child, you are a child, you are a child, and then you are not a child. What is your current thinking on that?

Dame Melanie Dawes: A lot of what we are doing is focused on harms that apply to all under-18s, such as—the law is very clear here—the requirement not to be shown pornography or suicide and self-harm material. I agree that our approach is not very nuanced towards the different ages beneath that. We have not said that this is appropriate for 16 year-olds, or this is appropriate for 13 year-olds and so on. That may be something that we are able to get more nuanced and sophisticated about over time. At the moment, our priority has been to get the basic protections in place.

Mark Bunting: I completely hear the point and agree with Melanie that this is something we will need to look at more over time. However, a lot of the harms we are worried about most when it comes to children are not particularly differentiated by age. We would be as concerned about 16 and 17 year-olds accessing suicide or self-harm content as we would younger children. There is a lot to do to deal with those harms for all children, while also developing a more sophisticated understanding over time of how they might affect different age groups differently.

Q27 **Lord Holmes of Richmond:** We have heard that the proposed crisis response protocols and recommender algorithm will fall short. For example, if they had been in place at the time of the horrific events at Southport and what subsequently happened online, they would not have had any impact. What are your thoughts on that?

Dame Melanie Dawes: We do not think that the Online Safety Act would have mitigated all the concerns we saw had it been in force last summer, which it was not.

I did see, from one of your earlier hearings, that there was some concern that Ofcom had overplayed the impact that the Act might have had. We would not want to overplay it. Misinformation and disinformation, for example, are not harms named under the Act.

However, when it comes to illegal content such as incitement to violence, had those events happened now, or indeed in response to the attack in Manchester a few weeks ago, we would have been able to ring them up, ask them what they were doing, confirm—once our measures were in place—that they had stood up their crisis response systems and were keeping an eye out for illegal content. A lot of that is going to be about talking to law enforcement and the Government, who are often closest to events, and understanding what the patterns are that need to be acted on.

The Online Safety Act makes a difference, particularly with the emergency response protocol, which we put in our additional measures consultation because of what we learned after Southport. It will make a difference, but it will never be able to completely mitigate the way that people behave online after an attack like this, which is pretty terrible

sometimes, with individuals bullying and behaving extremely badly online.

- Q28 Lord McNally:** It is interesting you said that, after Southport, you sent out inquiries over what they were doing. Is that normal practice? We were talking earlier about the attack on the synagogue, and we are likely to have other issues like that. Do you have in your procedures a warning system to platforms saying to them that this could be serious and asking for guarantees that they are taking appropriate measures?

Dame Melanie Dawes: Yes, and this is where our supervision relationships come in. I appreciate that the way we are implementing the Act, and the supervision approach we have set out with the largest companies, is not something we can talk about readily in public because we are having behind-closed-doors conversations with them in a confidential environment. However, after the Manchester synagogue attack, our supervision teams rang our contacts in the big social media companies to find out what they were doing. That is the sort of thing we will do in response to events like that.

- Q29 Lord Holmes of Richmond:** Taking you back to age verification, there is a significant issue around the accessibility or otherwise of the majority of technologies that are being used for age verification—for example, for those who do not have a smartphone or blind or sight-impaired people. How aware of this are you, and what action are you taking to address it and promote other means of age verification which may be accessible and available now?

Dame Melanie Dawes: It is something we need to keep looking at, and we take the point. This is very new for the industry, and the systems we have been recommending are still quite nascent. We want to make sure that we are doing as much as we possibly can to force the issues of accessibility across the system. We are happy to take the conversation forward outside today's hearing if there are particular things you are concerned about. It is an area where we need to do more work; we accept that.

- Q30 The Chair:** We are going to move on to questions about media literacy following on from our inquiry. Before we leave the Online Safety Act, can you clarify whether you are expecting to make further iterations or consultations on the codes?

Dame Melanie Dawes: Once we have concluded this particular set of measures—the consultation closes soon, and we will aim to have those concluded by next summer—our priority will be the enforcement of existing codes. Our inclination is not to do another set of codes too quickly, but it may be that there are measures that are effective, useful and address a risk that is not otherwise addressed. If that is the case, we will bring something forward. We have a lot of other policy work to do next year and the year after, including on categorisation and so on.

- Q31 The Lord Bishop of Leeds:** In our media literacy report we concluded

that “Ofcom is not the appropriate body to coordinate or deliver a nationwide media literacy programme”. Ofcom agreed with that statement. It “cannot deliver a comprehensive media literacy programme across the UK”. It is not the appropriate body and it “does not have the infrastructure to address these issues at scale”. The Government came back and said that “Ofcom, as the independent regulator, is well placed to lead delivery under its statutory duties in the Online Safety Act”. That assumes there is a gap. Who then takes responsibility?

Dame Melanie Dawes: We are clearly required to lead in the areas we have expertise in and that we are required to in legislation, but that can never be a comprehensive media literacy strategy in the sense of working out what needs to be in the curriculum and spending budgets. We do not have budgets to roll out programmes—it is just not what we do; we are a regulator. An overall comprehensive strategy would have to come from the Government, and indeed from the devolved nations because this is a devolved area. For the UK Government, it would be an England strategy, and it would be for the devolved Administrations to take theirs forward.

The Government are doing a lot of work in this area. They are drawing on what we have done at Ofcom over the last few years in developing best practice and building a good network, which is important. We are hoping that what we have done has given them some foundations.

Q32 The Lord Bishop of Leeds: Does Ofcom monitor the impact, particularly in education and public services? It seems that the Government are saying it is your responsibility, and you are saying the Government are doing a lot in this. Where is it being held together?

Mark Bunting: Our view is that there are two slightly different things here. There is a set of specific responsibilities in the Act that relate to our duties, including our role in convening platforms to improve their media literacy activities and in specific areas such as the protection of women and girls, and misinformation and disinformation, where it is for us to lead, convene and work with stakeholders to trial approaches to improve media literacy. We set out our strategy on that two years ago, and recently published a statement of recommendations to platforms about how they can improve media literacy.

Media literacy can mean a lot of things, including areas where Ofcom does not have any remit, such as education. In those areas, as Melanie has said, it would not be for us to lead. The Government do a lot in this area, and the work on digital inclusion is part of this programme as well. That broader leadership role would not be one that Ofcom could fill, as the committee has said.

Q33 The Lord Bishop of Leeds: How does Ofcom ensure that the Government’s Digital Inclusion Action Committee and its fund complement rather than duplicate Ofcom’s existing networks and grants?

Dame Melanie Dawes: By working closely with them. I was told by our team this morning that there was a meeting last week—with that

committee and multiple government departments representing health, education, communities and others—to have that specific conversation about how Ofcom’s pilots, research or networks can be used by the Government and how they join themselves up, which, I know from my years in government, can be hard because there are a lot of different moving parts in the system. The will is there to try to join this up. We will do what we can to make sure that any pilots that the Government choose to run do not duplicate ones that we already have in train.

Q34 The Lord Bishop of Leeds: I am sorry to come back to a question I have asked you before, but this still bothers me. Does Ofcom have the capacity and the competences to deal with the sheer volume of expectation upon it?

Dame Melanie Dawes: Do you mean across the Online Safety Act and our remit more broadly?

The Lord Bishop of Leeds: Across the organisation, but particularly in relation to this. I am conscious that, all the time, more is added to Ofcom’s agenda. Unless it is going to constantly accumulate more people and expertise, there must be a limit to what is achievable. That raises a question about whether the expectations are targeted on the right body. That is why I am concerned when Ofcom says it is not competent to do this and the Government say that it is its remit. Can you see the problem?

Dame Melanie Dawes: I can. There are two parts to this. First, should Ofcom, even if we had loads of resource, be co-ordinating a national media literacy strategy? My answer to that question is no. We are a regulator. We can contribute research and expertise; as Mark said, we can contribute to making sure that platforms introduce the right systems, processes and so on. Where it is about the right support for the education system, the NHS and community activities, it must be for the Government to co-ordinate. They are the ones that have the budgets. We will never have that. I am very clear about that, and they are as well, to be honest.

On the more general question of whether we can manage Ofcom’s remit, which has grown, yes we can. We now have about 1,800 staff. That makes us a lot smaller than the Financial Conduct Authority and smaller than Ofgem. We have a big remit, but there is a lot of synergy. Relationships with the tech companies cut across networks, infrastructure, cloud and data centres, and new forms of AI, from an infrastructure perspective. We are building very complementary relationships around online safety.

It would be difficult for a regulator to do the online safety work without the background that we have on content regulation, working with the media and so on. For me, it fits together, but we need to make sure that it does not grow beyond what we think we can do.

I think the media literacy question is a slightly different one. It would not matter how big we were, I do not think it would be right for us to co-ordinate it.

Q35 Lord McNally: As I have said to colleagues before, I was on the Puttnam committee that set up Ofcom and we had a paragraph in there about media literacy. Looking back, I am not sure we had the faintest idea what we meant by media literacy. It has many tasks for many people. We agree with you that it is not Ofcom's responsibility. However, the vague sense that it is the Government's responsibility is always dangerous, because that means it is nobody's responsibility. In our inquiry, we have to find out who is going to take responsibility for a media literacy strategy for government. In the meantime, how are you holding platforms to account on media literacy?

Dame Melanie Dawes: What we have done recently is consult on a statement of recommendations, as required by the Act, for platforms. Essentially, it will be guidance on how they should enable media literacy in the way that they design their services. That was published only a couple of weeks ago, in mid-September. It is open for consultation now. It is guidance, so it will not be something we can enforce against, but sometimes that gives us more opportunity, as it has on the women and girls guidance that we will complete shortly, because it means that we can set the bar high for best practice.

You can see from the draft statement that companies—we have also made recommendations to broadcasters—should be holistic and think about how they factor this into service design and measure impact. They should be thinking about how they support users along the journey of being on their platforms, how they use nudges and information, how they facilitate user reporting and so on. That is work we have done already, and we will be following through.

Mark Bunting: It is worth saying that we have built some of this thinking into our codes, where we have identified that it is proportionate to require companies to take steps to protect users. For example, in the protection of children codes there are measures requiring firms to provide supportive information to children when they post or access content that might be harmful to them. We can consider more of those types of intervention over time. Although the statement of recommendations is voluntary, where we have been able to make an evidence-based case for it we have brought some of those ideas over into our regulatory codes as well.

Q36 Lord McNally: We have recommended that Ofcom shifts its focus towards longer-term and larger-scale research projects, rather than multiple short-term pilots. What is your approach to that? One of the criticisms from the industry is that these short-term things give it work to do without any real outcome other than the feeling that it is doing something. Particularly with media literacy, there is a feeling that there has to be something more substantial in train.

Dame Melanie Dawes: We agree that we need to get longer-term about some of our work. We have taken that on board. The pilots we have in train now, in Birmingham, Glasgow, Northern Ireland and Wales, are longer term. They are, inevitably, quite small-scale—we do not have the budget for giant programmes—but they are targeted. They are very much about supporting particular communities and trialling what works in helping people to navigate their lives online and get better value out of it. They are slightly longer term, and I hope will make a difference.

Q37 **Lord McNally:** What about the other side of the industry, big tech itself? It is massively in its interest to get a workable definition of media literacy, and how and where it should be applied.

Dame Melanie Dawes: To be honest, I am not sure it sees media literacy as something that is terribly important to it at the moment. The social media business model, in particular, runs on attention—on clicks and engagement. It does not necessarily have to prioritise the experience that users have, because the trade we are all making when we go online is that we give our data over for an advertising-led business model rather than money. That has led to the platforms being far too blind to the experience that their users have, and why we have the online safety problems that we have. It also means that media literacy is not something that, in the way we would understand it, it particularly prioritises.

There are some in the industry who get it, and we have had some companies sign up to earlier versions of media literacy best practice that we have produced. This new guidance goes further. Once we have finalised it, we will need to work out how we are going to hold the industry to account and spotlight who is and who is not following it.

Q38 **Lord McNally:** Do you think a media literacy levy would concentrate their minds?

Dame Melanie Dawes: It depends on why you would do it. If you wanted to fund large-scale education programmes then the Government would need to think about how they fund them and who they want to levy in any sector of the economy.

We already have platforms paying for Ofcom's fees as the regulator, so they are already paying for our media literacy work because they will be paying fees during the course of the next financial year to us—that is coming in shortly. If the Government wanted to go further then they would need to think about that as a broader question, and I am sure the Treasury would be very interested.

Mark Bunting: There can be a downside to levies, in that it enables companies to say that they have paid their debts by contributing to a levy. In the case of the big platforms, we want them to do more to embed media literacy and online safety thinking into the heart of the business and not think that it is something they can deal with by paying a bill once a year.

The Chair: Maybe both.

Mark Bunting: Or maybe both.

The Chair: That is our position. That is a good point to finish on. Thank you very much for answering all our questions today and for your evidence.