



Speaker's Conference

Oral evidence: Speaker's Conference on the security of candidates, MPs and elections, HC 570

Wednesday 3 September 2025

Ordered by the House of Commons to be published on 3 September 2025.

[Watch the meeting](#)

Members present: Sir Lindsay Hoyle (Chair); Mr Clive Betts; Samantha Dixon; Zöe Franklin; Dr Rupa Huq; Ben Obese-Jecty; John Slinger; Sir Mark Tami; Sir Jeremy Wright.

Questions 346 - 390

Witnesses

I: Jessica Zucker, Director of Online Safety Policy, Ofcom; Almudena Lara, Director of Online Safety Policy, Ofcom; and Mark Bunting, Director of Online Safety Strategy, Ofcom



This evidence includes content that some may find distressing

Examination of witnesses

Witnesses: Jessica Zucker, Almudena Lara and Mark Bunting.

Q346 **Chair:** First of all, welcome. I don't know if you would like to do a quick introduction. It would be very helpful.

Jessica Zucker: I am Jessica Zucker, Policy Development Director at Ofcom in the Online Safety Group.

Mark Bunting: I am Mark Bunting. I am the Director of Strategy Delivery in the Online Safety Group.

Almudena Lara: I am Almudena Lara and I am the Policy Director with responsibility for child safety.

Q347 **Chair:** Welcome. Just as a reminder, what level are you within—how many people are above you?

Mark Bunting: We are directors in the Online Safety Group. That group is run by Oliver Griffiths, who joined a few months ago, and Oliver reports to Melanie Dawes, who you will be familiar with and has come to present to Committees plenty of times.

Q348 **Chair:** Do you feel you are the right level for this important Committee?

Mark Bunting: I think across the span of responsibilities that you have here, we can cover the questions that you have for us, yes.

Q349 **Chair:** Not quite the answer, but I know what you mean. I am just asking: did they feel that it was not appropriate for somebody else more senior to come?

Mark Bunting: The decision that we took was that the best use of your time and ours was to send people who had the relevant expertise to answer the questions.

Q350 **Chair:** But it is not downgrading this Committee?

Mark Bunting: It is not downgrading this Committee, absolutely not.

Chair: Okay, we will make a judgment at the end, won't we? In which case, I will hand to Sir Jeremy.

Q351 **Sir Jeremy Wright:** Welcome all. We have had these conversations before, but let me ask you each to think about some of the implications of the Online Safety Act for Ofcom. I think this will probably apply, unless Mr Speaker tells me otherwise, to all the questions. Please don't all feel you have to answer every question, but I will ask these questions and whoever you think is best to answer, please do.

The first question I want to ask you about is the degree of change that you think the Online Safety Act will bring, and particularly what you look to bring about from an Ofcom perspective. I am interested in hearing about the degree of shift that you think the Act will bring about in the



HOUSE OF COMMONS

This evidence includes content that some may find distressing

behaviour of the platforms. You will understand our particular remit here is to think about the impact on MPs, candidates and the political world more generally. Secondly, give us some indication of how confident Ofcom is that it has the powers and resources it needs to bring about that desired change.

Mark Bunting: Shall I kick off? I very much take the point that the main focus of the Committee today is the safety and security of MPs and elections. I will ask Jessica to come in on that in just a minute, but perhaps it would be worth setting out some broader thoughts on where we are with implementation.

It is a little less than six months since the online safety duties came into force. We wrote to the industry at the start of the year, shortly before the illegal content duties came into force, setting out the areas where we thought immediate improvement was needed. There are five of those: improvements in the governance and management of risk by online services; action to prevent the distribution of child sexual abuse material online; the wider use of age checks to ensure that children could be shielded from harmful content without infringing adults' ability to access that content; rapid removal of illegal content when services are aware of that content disseminating on their platforms; and the transformation in children's online experiences, particularly with respect to the way that algorithms have played a role in delivering harmful content to children.

Those are big missions. I don't think we are under any illusions about the scale of the task there and of course this is an industry that has not been regulated in this way until very recently. Where we are now is that we have been reassured by the reaction to the early interventions that we have made. We have gathered around 70 risk assessments from the services that we think pose greatest risk to people in the UK. That is on the illegal content side and we are now going through a similar process on the protection of children side. That has given a really comprehensive picture of risk in the industry. We will be publishing a report later this year that sets out some of the insights that we have gained from that process.

I will not go through all five goals in detail now, but it is clear to us on the first goal that there is still a big gap in companies' governance of risk and the ways that they think about the risk in operations and product designs. We have seen some immediate improvements and particularly the deployment of age assurance after 25 July when the protection of children measures came in has been very positive. We have seen quite widespread compliance with those rules, but there is still a lot to do, particularly in the areas of illegal content takedown and protection of children from harmful content distribution via algorithms. It is early days. We are pleased to see some immediate change in line with the duties, but clearly there is a very long way to go.

Briefly on the last part of your question, Sir Jeremy, we feel that the Act gave us a comprehensive suite of powers to tackle the problems that the



This evidence includes content that some may find distressing

Act identified. Some of them are still to be proven. For example, the end road of the enforcement process for us, when we can't get compliance with the codes, is to apply to the courts for measures to prevent services being available in the UK. We hope we don't have to use that very often but it is an important shot in our locker. That is currently unproven and we will want to see that we can use those powers effectively if and when we need to. In some areas, yes, of course, there is still more to do to understand where the change is needed.

Q352 **Sir Jeremy Wright:** I know that Jessica wants to come in, but I will ask you very specifically about illegal content. You will understand that our concerns are slightly broader than what is a contravention of the criminal law but obviously contraventions of the criminal law are a significant part of what this Committee is concerned about. As you know, one of my concerns about the way in which the Act is being seen at the moment is whether or not it as easy as it should be to work out what illegal content actually is, particularly where a particular mens rea is concerned. Some of the new communications offences that will have particular relevance to us as MPs require, none the less, either intent or recklessness. Is it in your view appropriate to expect the platform to understand that mental element to come to the conclusion that that content amounts to an offence, and that is what the Act requires, and thereby take it down? If not, what else needs to be given to them to enable them to make those judgments?

Mark Bunting: There are a few aspects to that, and again I will bring in Jessica in a second. We have said that companies need to have reasonable grounds to infer that content is likely to be illegal. That does not mean they need to have evidence of the mental state of the individual who has posted the content. In many cases the context is reasonably clear and sometimes the words themselves are sufficient to judge that an offence is likely to have been committed. Our focus is on the areas where there is greatest evidence of harm and greatest capacity for services to act. Where there is clear incitement to violence, threats to kill, encouragement to commit suicide, those are areas where companies do take steps. They have trained teams to identify and assess that type of content.

Will that always be black and white? No, clearly it is not and there will be a very wide grey area. My sense is that in the particular areas that you are looking at sometimes that context will be very difficult to identify and we will learn more as we go through the process.

Q353 **Sir Jeremy Wright:** That is exactly the point. What I am slightly worried about here—again feel free, either of you, to comment on this—is that these logics become somewhat circular. You are right: you will be entitled to ask that platforms consider whether they have reasonable grounds to infer this but what they have reasonable grounds to infer is whether content amounts to an offence. It only amounts to an offence if both the physical and the mental element of the offence are present. What I am



HOUSE OF COMMONS

This evidence includes content that some may find distressing

worried about here—tell me I should not be—is that you will default, as regulators, to saying that unless it is obvious on its face that an offence has been committed, we will not expect the platform to take it down. Is that the position?

Mark Bunting: I would start somewhere else because our job is not to opine on individual items of content. Our job is to make sure that companies have the systems that they need.

Q354 **Sir Jeremy Wright:** Sorry to interrupt you. The systems they will apply will be based on the expectations that you, as the regulator, have set. That is the way it works, as you well know. You have been busily constructing your codes of practice because we, as legislators, have handed to you responsibility to set out what compliance with the Act really means. We are entitled to ask you, surely, what you think compliance with the Act really means. In this context, when we are talking about illegal content, material that might be aggressive beyond the point of acceptability under the criminal law where MPs or candidates are involved, it looks to me as though there is at least a danger that we will end up saying we can only really ask the platforms to have systems and processes to take this content down when it is obvious on its face, without consideration of the mental element, that an offence is being committed. I just want to know if that is your sense of it.

Mark Bunting: The way that we will go about doing that is by talking to services about how their systems work. If we think about this from the companies' point of view, they have a range of ways of identifying content, including some automated tools and human detection in taking reports from law enforcement, interested flaggers and so on. The question we will ask is how have they gone about the process of assessing whether or not an offence is likely to have occurred. I don't think it would be helpful for us to say up front where we think the line should be drawn for the standard that they are applying. The automated tools do not make any judgment about the mental state of the poster and companies will routinely take down content without knowing much about the mental state of the poster.

We will want to understand how they are assessing whether they have caught stuff that is likely to be an offence and not caught stuff that is unlikely to be an offence because, of course, that is where the free speech considerations come in. Every platform will do that and our first question is: are they going about making that judgment in a careful, considered and systematic way that is capable of being scrutinised by us as the regulator. We do get to your question but I think we get to it after quite intensive scrutiny with the platforms about how they are making their judgments.

Q355 **Sir Jeremy Wright:** Understood. Jessica, I know you want to come in on this.



HOUSE OF COMMONS

This evidence includes content that some may find distressing

Jessica Zucker: Thank you again for having us here and the opportunity to give evidence in this session. I want to talk a little bit about the specific subtopic in here of how we are thinking about safety and security of MPs and candidates and elections, which is obviously very important particularly with the upcoming elections next year in Scotland and Wales. We thought we would share a little bit about how we see the risks and threats here and a little bit about what we are doing and then would welcome the opportunity for any questions on our approach.

The ability for politicians to be able to engage meaningfully online without fear for their own safety, their families' safety and their livelihood is absolutely integral and central for a strong democratic system. We couldn't agree more. The research that we have been doing shows some worrying trends, however. For example, issues around hate and abuse particularly targeting women in politics is getting worse over time and has really detrimental impacts on their livelihood and their choices to even enter politics. It is something we are extremely aware about.

Q356 **Sir Jeremy Wright:** It may be helpful for you to know that we will come to this with some separate questions. Perhaps if I can ask you just to limit yourself at the moment to the question that I have asked, which is about the expectations that Ofcom has for success. What are you looking for platforms to do by way of change? Do you think that powers and resources are adequate under the current allocation for you to do that successfully?

Jessica Zucker: I don't want to repeat what Mark has already covered, so specific to this topic I will limit it to what we expect now and in the future. On what we expect now, much of the hate and abuse directed towards politicians clearly falls into illegal offences under UK law. We have talked about some of those already. We have given some pretty clear guidance and examples in illegal harms codes of practice. In these cases we will not hesitate to be holding platforms to account to ensure they have terms of service that reflect these, content moderation systems that are effectively trained and resourced and these are reporting in appeal systems.

That said, some of the hate and abuse that we know people in politics get does not constitute an illegal offence despite how harmful it might be still. In these situations the Act does not require platforms to restrict access to that kind of content unless it is being served to children. Where it is being served to children, we will take enforcement action if needed and work with companies to promote compliance.

Lastly, a forward-looking thing that we are working on is that some of the larger services will have additional duties in this space. They will have to give their adult users additional tools to be able to choose what kind of content they see that might fall into this category of harmful but legal content. They will have the ability to filter out certain forms of legal hate and abuse as well as filter out content from non-verified users. This is



HOUSE OF COMMONS

This evidence includes content that some may find distressing

some of the stuff that we are looking forward to in the future that I think is relevant to the discussion here.

Q357 Sir Jeremy Wright: Just one more from me. You are right, of course, that the Act in its current form does not include anything beyond material that is harmful to children or illegal content. I suppose the only area where that might not be true is when we come to the categorisation process and we talk about the powers given to users to control their own interactions online for category 1 providers. Again on your expectations, can you tell us what success looks like for the usage of those powers? Do you expect to see a certain level of take-up of user empowerment powers? The reason I am asking you that is you will appreciate from a parliamentarian or a candidate's point of view, it is quite a difficult ask to say you are, of course, entitled not to interact with the people you are representing or hope to represent. That is a big decision for a politician to make. What is your expectation of what success looks like when those powers are available by way of how they are used by those in politics?

Jessica Zucker: This is precisely why we have done some recent engagement with people particularly in high-profile positions because the kind of tools that they will want to use may differ from me, Mark and Almudena. There are blunt instruments that may not be the obvious choice for people who want to maintain that level of engagement. I will start by talking about some of the research and then what we are looking to do.

We conducted two wide reports where we interviewed in a qualitative way high-profile public figures in sports but also recently women in politics. We asked them questions about the kind of hate and abuse that they receive, the kinds of tools they are using today and why or why not they are effective. Some of the things that we learned precisely was that, that some of these people don't want to have to entirely cut off access to the people they are trying to engage with. We developed a more nuanced understanding of the kinds of tools that people in high-profile positions might want to use.

Rather than having a way of filtering out all types of certain content where you might then be less aware of what people are saying about you, the threats related to you, you might be able to take other actions such as having a different type of ranking, the most harmful content in a comment may not be showing up at the very top of a post but may be towards the bottom, being able to limit the type of interactions that you have with people or even things like having warning screens over different forms of content. There is a wide range of a different variety of tools that fall into this space.

As you know, we are in early days of policy development here, so I can't give you the full range of options that we are considering but I can assure you that we are looking this space and trying to ensure that our proposals will work not just for people with high-profile online presence



HOUSE OF COMMONS

This evidence includes content that some may find distressing

but also for people like myself and others who might have a different set of risks and interests in their engagement.

Sir Jeremy Wright: I could talk about this all afternoon, but I won't.

Ben Obese-Jecty: A quick question from my perspective. You mentioned MPs who receive an awful lot of abuse. I have noticed that the tone in the nation has shifted in the last month or so and the amount of racist abuse I have received personally has just gone off the charts.

Chair: These are Rupa's questions that we are coming to.

Ben Obese-Jecty: Sorry.

Chair: You can come in on the back of Rupa's questions. That would be very helpful.

Dr Huq: I think it has already been answered.

Chair: I am sure you can get something out of it.

Q358 **Dr Huq:** The headline from *The Guardian* this recent bank holiday Monday was "MPs voice alarm at the rise in online abuse" over the immigration debate. It seems that we are seeing a quite contrasting picture in what the social media platforms say. They all have very positive reports—we had them in our last session here—from their transparency reports and they say that negative experiences are going down but Ben has been saying—and there is the horrible case of Anna Dixon over that bank holiday weekend. In her situation it was a neighbouring Tory MP trolling the Labour MP with a misleading video that then led to death threats and the police coming round. There is a big mismatch between what the platforms are saying and what we are all experiencing.

What do you think? How does Ofcom perceive the current atmosphere on social media platforms towards elected officials? How useful are the transparency reports when it is a bit of a judge and jury thing, is it not, in assessing whether regulation is leading to a safer experience?

Jessica Zucker: I am happy to kick off. Our research paints a different picture than the ones that social media companies might be offering. I started with a couple of stats where we are very aware about the issues, particularly targeting women in politics but also people from backgrounds of protected characteristics. This comes up time and time again in our research, qualitative understanding the depth of the impact, as well as quantitative.

Some of the research that we do year on year tracks people's experiences online and one of the key findings that really stuck with me is that misinformation in particular is one of the most widely commonly referenced online harms that people experience. In our online nation report last year, people said that was about 40% of the overall online



HOUSE OF COMMONS

This evidence includes content that some may find distressing

harms landscape. The research we did on the election period last year indicated that there was a small but significant uptake of electoral and political misinformation after the election was called. There is a really obvious correlation there.

It is also worth mentioning that in the last few months we have seen technology developing in a really rapid way. That means that we will need to be really careful in thinking about what that means for AI and deep fake technology in the next election. That is why we have been doing quite a lot of research in this space to understand how it manifests, what we might be able to do on the media literacy side to help people prepare for it as well as better understand the kinds of mitigations that we can recommend that platforms take up.

Almudena Lara: If I can add to this because in addition to the protection of children, I also lead the work on women and girls. Obviously there is a lot of intersectionality in the harms that MPs suffer and if you are a woman and if you have other protected characteristics you are obviously much more at risk of online abuse. We are working to publish our final guidance to services, setting expectations on what to do and how to better protect women and girls, by the end of this year. We have gone out for consultation covering four specific types of harm that we see particularly affecting women and girls: the proliferation of misogynistic content, the pile-ons and harassment that women suffer, especially women in high-profile and political roles, the abuse that women and girls suffer particularly from the sharing of intimate image abuse—and, as Jess said, that is proliferating even further now with GenAI—and online-enabled domestic abuse. Those are the four areas where we are setting clear expectations for services on foundational steps that we expect them to take as well as good practice that we expect them to address.

Q359 **Dr Huq:** Are these transparency reports enough? How will you assess the adequacy of whether the platforms have the resources to deal with content moderation? Ofcom was set up over 20 years ago as a broadcasting regulator, the airwaves, TV and radio and I think it is also responsible for postal and telecommunications. I don't know how you can cope and I don't know how these platforms can cope either.

Jessica Zucker: Today platforms don't have to do transparency reporting. Some of them do. Before the Online Safety Act, platforms could do voluntary transparency reports if they wanted to and many of the largest ones have but they have done it of their own voluntary accord and no one is checking their homework. The Act puts new responsibilities on categorised services to have to comply with Ofcom transparency requests.

Once we finish our categorisation register, my team will be issuing transparency notices to categorised companies that will lay out in very specific detail all the datapoints and qualitative points of understanding that we expect them to then have to publish. Ofcom will take all of those transparency reports that the platforms will have to publish and we will



HOUSE OF COMMONS

This evidence includes content that some may find distressing

write our own report that makes sense of it and communicates our findings, shining light on the best practices, any areas that we think can go further. I think this will be one of the most important tools that we have in our regulatory toolbox. As I said before, platforms could put out whatever information they wanted to but we will have the power to ask them questions about the efficacy of their content moderation systems, their policies, the impact that they are having on user safety. I think that this is where we will see a real difference.

Coming on to some of your other questions, from my perspective, because I oversee a lot of the work around free expression and how you balance safety and rights, having a background regulating in broadcast has been really helpful. Unlike our broadcasting team, the Online Safety Group, as Mark said, is not sitting there making decisions about individual pieces of content, but because our broadcasting team has that experience of carefully balancing the broadcasting code and thinking about human rights law, we have integrated some real expertise in our group and understanding fundamentally how you balance these tricky issues. We have also done quite a lot of recruiting to make sure that we have the right skills and talents. Almudena and I both come from backgrounds having worked in the tech industry and I think that is important to the work that we do today because it is informed by real expertise.

Mark Bunting: Building on that and going back to what I said at the beginning about the scale of the challenge here, you asked about our resources and the capabilities of industry. The reason we are so focused on these questions about how companies think about risk and how they embed these considerations in their day-to-day decision making is because in the end that will be the thing that drives substantial and sustainable change in these areas. We will use a combination of engagement with industry to make sure they understand the rules and to enforce them when they don't comply, but in the end we have to see voluntary compliance and we have to see a return to a focus on safety in the industry, which I think probably in some areas has gone backwards over the last year or two, and of course that is a concern to us.

Regulation has an important role to play by establishing clear expectations of disclosure and the core standards of effective trust and safety practice in industry. We have started to do that but it will be a long road and it is a road where we have to take industry with us through that mixture of persuasion and influencing and constructive collaboration, plus the hard edge of enforcement when we need to do that. As I said right at the outset, we think we have made a good start with that but we are under no illusions about how much more there is to do.

Q360 **Dr Huq:** The Act says that platforms should remove illegal content swiftly. How do you define "swiftly"?

Mark Bunting: We have seen some jurisdictions set specific time limits for those things. I think that is a bit dangerous because if, for example, you set a target of 24 hours, that might be fine in some cases but it



HOUSE OF COMMONS

This evidence includes content that some may find distressing

might be far too long in others. The Act puts the responsibility on platforms to have the right systems to make the right judgments at the right speed about different types of content. When we see events happening very rapidly—and I am thinking here, for example, about some of the protests we have seen this summer and even more so last summer—we expect companies to act very quickly when they become aware of illegal content circulating. They have to be case-by-case judgments and that is the work that we are engaging with them on at the moment.

Q361 **Zöe Franklin:** I was interested in one of the comments you made earlier—I think it was Mark—when you talked about something being often not illegal but clearly very harmful. Thinking about the report you signposted to, I have read it and I think it is a really depressing read, particularly from the perspective that women are actually self-censoring rather than the platforms dealing with the issue of not illegal content but, frankly, unconscionable harmful content. How is Ofcom planning to tackle this gender-based harm and misogynistic abuse to help change the way this is working? It is unsustainable for women in politics.

Mark Bunting: I think my colleagues might want to say a bit more.

Almudena Lara: I spoke about the guidance that we have published for consultation and we are working to publish in final form at the end of the year. Our evidence is completely in line with the experience that you have described. There are elements of the illegal harms codes of practice and the protection of children code of practice that already set limits to what services can do and what they should be doing to protect women and in particular women in politics. For example, the distribution of intimate image abuse is illegal and that should be suppressed and companies should take that down. We have also stretched those expectations further by now we are consulting on the use of technology for the proactive detection of bad content so that it can be taken down swiftly as soon as it is identified, that companies make the effort in identifying this content.

We are working as well, when we talk about pile-ons and harassment, with companies and we have heard good practice from companies about how they can de-escalate some of that content that they see coming often from a very limited number of accounts that are creating a lot of volume of engagement and how they might use the algorithmic design to de-escalate some of this content and also how they can give women wider user tools to help identify and manage that content and experience.

I am terribly sorry. We all work really hard to try to make things better. The situation is obviously unsustainable, from the research and evaluation that we have been carrying out, as you say.

Mark Bunting: A quick thought, Almudena's reply has highlighted something I should have mentioned in response to Dr Huq's question. I think that the goal here has to be earlier and proactive identification of



HOUSE OF COMMONS

This evidence includes content that some may find distressing

this content, not waiting for users to report it and take it down. In some areas there are technologies already widely available and used by the industry but they are not universally used and the accuracy and effectiveness of those tools is not always transparent. A big focus for us will be can we get wider use of those tools and can we be confident that using those tools to remove content before it is seen by anybody is effective at removing the illegal and harmful content without inadvertently catching all kinds of legitimate speech. Of course that is right at the heart of the debate that we have seen over the last few weeks about the balance between free speech.

I anticipate that those tools will get better over time and will be able to be deployed more widely by a wider range of firms, including as AI helps to improve those tools further. That will be a big focus for us and, as Almudena said, we are consulting on that at the moment.

Q362 Ben Obese-Jecty: It is interesting to hear the steps that Ofcom plans to take. To Zöe's point, I receive a huge amount of abusive and very unpleasant content and the last four weeks have shown that that has gone off the chart. I must have received hundreds and hundreds of comments, many of which are just simply very unpleasant, they don't meet the criminal threshold. They are not something you would want to see but they are not something that anyone will be prosecuted for or even have a slap on the wrist about, but some of it is simply outright racism and criminal. A selection of Tweets I have received recently: "Cry about it, you dirty nigger"; "Shut the fuck up, nigger"; "Shut it, obese nigger"; "Boo hoo, nigger. Welcome to the world of free speech." Those are all posts on X.

They require me to report them and even when I have reported them, there is almost no confidence that they will be removed. If one has used effectively a foreign use of one of the letters that has an accent on top of it, that will bypass the moderation. There is no physical or human moderation of those tools. To remove it before I ever see it is almost wishful thinking. I talk about X specifically because other platforms simply do not have this problem to the same degree.

At what point will this cross your desk as Ofcom in a way that the company then receives a reprimand from Ofcom or a fine? How will you deal with the sheer volume? I am one person and that is several instances. Are you in any way scaled to deal with the deluge of examples that you should technically be sent? Is this something that you would use AI to be able to process? Is there a risk in that? How will you get to a point where the platforms are actually responsible for the racist content that they have on them? At the moment, I just get pelted every day and much as I would love to sit around blocking everybody all the time, I should live in a world where I simply am not racially abused.

Mark Bunting: I will kick off and Jess might want to come in. The first thing to say is we are all too familiar with stories like that that you have just described to us. Of course that abuse has no place in a civilised



HOUSE OF COMMONS

This evidence includes content that some may find distressing

society. Sadly, it is far too common. I am not going to get into the specifics of particular platforms but in my experience platforms that are lax on handling speech of that kind also tend to be relatively lax in handling of illegal content. Their moderation systems will apply across all the types of content that they are supposed to be acting on.

Our focus has to be on the illegal end of that and of course some of the content that you are seeing probably does cross the criminal threshold, I would imagine. Where our focus has to be on that, we have the tools to scrutinise how effectively those content moderation systems are working. It does not require us to be collecting millions of examples of that type of content ourselves. It requires us to be able to forensically interrogate what a company is doing.

We have started doing that work. Of course, it is early days. We are focusing intensive investigations on the services that are biggest and, in our judgment, pose the greatest risk of carrying this type of content. Right now our focus is more on the reactive response and the handling of complaints. Companies have to have effective complaints processes and they have to provide appropriate feedback to people who have complained. Where we have evidence that that is not working, we can take that evidence into account. As I said earlier, from next year we will be able to focus more on the automated detection piece as well.

Absolutely, although we cannot engage directly with the legal dimensions of that, I hope and anticipate that where we drive improvements in content moderation efforts is beneficial on the legal side of the divide as well as the illegal side.

Almudena Lara: If I can add to that, a big plank of the system is the risk assessment, as Mark said. If companies continue to receive this type of content, if there is evidence externally—and there is research and there are organisations consistently collecting this data to prove that the company or the service poses a high risk of this type of abuse—that is evidence that needs to be taken into account by the company and will help us to hold them to account for the risk that they are posing to users.

Jessica Zucker: I will add a couple of other quick points to this. When thinking about whether a content moderation system is sufficient enough, one of the things that we might be looking at is whether it is properly trained. From my experience, having worked in industry before, that means that you need to have human moderators, automated systems that can take account for the things that you mentioned—misspelling, strange spelling, replacing letters with numbers, using emojis in place of words. Those are all the kinds of things I think we would expect a highly trained and effective moderation system to include and it is something that we can certainly take a look at as we are thinking about compliance with our current measures.

When it comes to legal but harmful forms of content, as Mark alluded to, this is where I hope to see difference being made in the category 1



HOUSE OF COMMONS

This evidence includes content that some may find distressing

duties, which are not in place today and I think will make a difference once they are. I mentioned some of them earlier where there will be additional tools that adult users can use to filter out certain types of content or not have to engage with people who are not verified. Those will make a difference in some aspects.

The other area is that category 1 services will have a duty to apply their terms of service consistently. They don't have to today and some potentially categorised services will require the moderation systems to go further than what is defined as illegal under UK law. They may choose, for example, to have a wider definition of hate speech to include both illegal and legal forms. Where they decide to set those lines, if they say that this is banned in their terms of service, we can make sure that we are holding them to account to enforce the terms of service consistently, which I don't know that they are today.

Q363 Sir Jeremy Wright: I want to track back, if I can, to what Mark said about proactive tools that might be available to the industry to make sure this content is not there in the first place, which is what we are all hoping to achieve. With the structure of the Act, as you are well aware, and the importance of the codes of practice, it matters hugely whether you include in the code of practice the use of these tools. If you do, because of the safe harbour the code presents, it is high likely that platforms will use them. If you don't, they may take that as a signal that that is not the sort of thing you are looking for. The question I ask is: what are your thresholds for including these tools as recommended usage in your codes of practice? Are there any obstacles to doing that around particular IP licences or particular individual products? Do you have to be more circumspect than that? What are you looking for to be able to include that in the code of practice, which seems to me to have huge force?

Mark Bunting: We are consulting on that at the moment. The approach we have taken is to propose that services should use those proactive detection tools for certain categories of content, particularly some of the key offences like terror content and child sexual abuse material but also the types of content that are harmful to children.

Q364 Sir Jeremy Wright: Are you talking about hash matching technology and the like?

Mark Bunting: Hash matching will be part of it but the other aspect of this that we are consulting on is the use of tools to automatically detect new versions of that content. Hash matching is good at catching previously identified content that has been validated as being illegal or harmful, but the new tools will allow detection of new content, for example nudity filters, tools that can automatically identify nudity in images and then assess whether that nudity is likely to be somebody who is under 18. That is one step further than the hash matching that we have proposed previously. We are also extending that to detection of content that is pro suicide and self-harm and pro eating disorders. That captures a lot of the material that is harmful to children.



HOUSE OF COMMONS

This evidence includes content that some may find distressing

The proposal is that the codes of practice will say that big services and services that are risk of those harms should use those tools subject to them doing an assessment that the tools are sufficiently accurate and effective. The reason we have built in that condition is because we don't want the use of those tools without verification that they are adequate for the job that—

Q365 **Sir Jeremy Wright:** Are you expecting them to do that verification rather than you doing it?

Mark Bunting: We are, because every company may want to take its own approach.

Q366 **Sir Jeremy Wright:** If a platform says, "I haven't used it because I don't think it is accurate," do you simply accept that or have you a way of verifying whether that is a reasonable argument?

Mark Bunting: Yes. We will scrutinise the assessment that they have made of accuracy and effectiveness and obviously if we don't agree with it they—

Q367 **Sir Jeremy Wright:** You will need to be in a position to assess the accuracy of each of these tools to do that.

Mark Bunting: We are getting into the weeds here, but we will probably validate the quality of the test that they have done. We will not necessarily repeat the test ourselves.

Q368 **Sir Jeremy Wright:** These are important weeds because, as I say, there is a difference between inclusion in the code of practice and not. If what you include in the code of practice is simply an expectation that people will use a tool that they themselves think is an accurate tool to use, that is only of value if you are prepared to say. "That wasn't a reasonable excuse because it is an accurate tool in our view and you should have used it." I want to just clarify that you are prepared to do that.

Mark Bunting: We will be in a position to do that. Almudena, do you want to add anything to that because you have been involved in some of that work?

Almudena Lara: Not at this stage, but I acknowledge the point that you make that we need to be in a position to be able to hold them to account and we have a team of technologists working at Ofcom that will look into that.

Q369 **Samantha Dixon:** I want to pick up on the comment Mark made about the fact that Ofcom can't engage on the legal side of it. X has increasingly higher thresholds for removing abusive or threatening content and has refused requests for information from the police to identify perpetrators. X has told us that, "to be able to disclose information, we are in need of evidence". Is it appropriate for them to be making their own assessment of when to comply with requests for information from law enforcers? Is X in breach of the Online Safety Act regulation if it fails to comply with



HOUSE OF COMMONS

This evidence includes content that some may find distressing

requests from law enforcement and in the context of what you are saying about enforcing their terms of service?

Mark Bunting: The main focus of the Act is on identifying and ensuring the rapid removal of illegal content and the purpose of that clearly is to ensure that users are not routinely exposed to it. That is our primary focus. The engagement with requests from law enforcement is relatively narrowly drawn in the Act. There is one area, which Almudena can say a little bit more about if that is helpful, where services have to report incidences of child sexual exploitation offences on their service. We have also recommended that in the event of a national crisis where there is a significantly heightened risk of illegal content being distributed, they should have channels of communication with law enforcement to understand those risks and to take appropriate action. But the Act does not envisage and does not give us powers in most cases to require services to do more to engage with law enforcement beyond their existing duties to do so, which will come up in other bits of legislation. There are some areas where we have more teeth to secure improvements there but they are limited to particular cases.

Q370 **Samantha Dixon:** I think it is less than 50%, less than that, which given what Ben has just outlined, which is clearly illegal or would appear to be, is really quite disappointing to hear.

Mark Bunting: Yes. I agree with that. Our powers would be limited except in the areas that I have mentioned. The other area that is not really relevant to what you are describing but for completeness, coroners have the power to ask us to request information from services. Those information requests, like all of our information requests in pursuit of our own duties, are enforceable and we can impose sanctions if companies don't comply with those requests. We have done that on several occasions, particularly in the video sharing platform regulation that preceded this, but that is our requests for information not law enforcement requests.

Q371 **John Slinger:** We took evidence from Patricia Rossini, who is a lecturer in political communication, media and democracy at the University of Glasgow, who you may be aware of. She made clear that the platforms are not transparent and it is interesting because you were talking a lot about transparency but they are not transparent in the ways that they are using recommender algorithms to drive further engagement. How much access will you have as Ofcom to the information that they possess about how their platforms design those algorithms to manage the content and engage their users?

Jessica Zucker: The Act, under section 100, gives Ofcom the powers to be able to request certain types of information from platforms to exercise our regulatory functions or to decide whether to exercise those functions. This might include asking for information about how the recommender systems work or their algorithms work in some cases, which I think will be, quite frankly, complicated and challenging to do, but we also have the



HOUSE OF COMMONS

This evidence includes content that some may find distressing

power to request real-time access to seeing how some of those systems and processes work in practice. We have the ability to get that information should we need it.

What I also think will be quite useful here—again going back to our transparency reporting powers—is the first set of powers I just mentioned are for information that the regulator can receive to decide how we want to exercise our powers but the transparency reporting functions require platforms to put information out to the public. This is particularly helpful to empower the research community to make sense of the huge, vast amount of information that is published every day about platforms. This is where my team will be looking at all kinds of questions about the way that algorithms work, the reach and impact, what kind of content is being recommended. This is what we will be looking at to understand how we can ask the right questions so that we are, for the first time, forcing them to have to put information out there about how their systems work.

Q372 John Slinger: Thank you for that. What sanctions do you have should you suspect that they are not revealing enough information? They are not going to give you IP, I guess, but what can you do if and perhaps when they try to withhold information, given the public concerns and the concerns of many parliamentarians about the way that they use algorithms to drive particularly dangerous content to maybe vulnerable people?

Jessica Zucker: All information requests, whether it is the first category that I mentioned or the requests that we make for—they really are not requests, they are mandates, so this is information that you have to publish. Those are enforceable. Should a platform choose to ignore an information request or choose to ignore transparency notices, those are offences that we can easily enforce against them. In fact, we have done so in the past under, what Mark mentioned before, the video sharing platform regulatory regime. We have taken enforcement action in situations where platforms in some cases ignored or rather inaccurately responded to those official requests for information.

Q373 John Slinger: Thank you for that. That is very helpful because the way that those algorithms operate when it comes to this particularly difficult issue of what is free speech, what constitutes appalling racist abuse, such as what Ben has to endure, the kind of attacks and intimidation that we receive often as Members of Parliament will be affected, I imagine, by the way they are using their algorithms. We would be very glad to hear as much as possible about that particular subject.

Mark Bunting: I completely agree. The other thing that might be worth mentioning is that we have also included in our codes of practice recommendations that to comply services should test their algorithms for unintended consequences, including surfacing illegal content or harmful content to children. I think that will be an important tool for us to be able to scrutinise those tests and, first of all, verify that they are taking



HOUSE OF COMMONS

This evidence includes content that some may find distressing

appropriate action in response to them but also just getting a better sense of how big that problem is.

Almudena Lara: If I can add to that, one aspect of it is how the algorithm is being designed and how it operates from a technical point of view, but at the end of day, for example when we are talking about protecting children, it is about what the experience is of the child when they use a social media platform. We have quite good baseline data about how easily they are currently being exposed to harmful content and we can test how their experiences evolve as the duties come into force to see whether that experience is changing. That will also give us an insight into how the algorithm is working in practice.

Q374 **Mr Betts:** Just moving a little bit ahead, presumably you are thinking about phase 3 of the Act implementation when service providers will have to provide user empowerment features and user identity verification options. I presume you are already talking to the main providers about how they will do this and comply with the legislation when it comes into effect. Do you expect them just to willingly give you everything you would expect or will you have to use enforcement? If so, are you already thinking about the enforcement you may have to use?

Jessica Zucker: I am happy to take that one. These duties are not yet in effect. We are at the very beginning stages of developing the policies around that and the reason for focusing on that now is we have been focusing on our implementation of the first two phases of the Act, protecting people from illegal content and protecting children. To proceed with publishing our proposals in this space, we first need to identify which companies will be subject to the additional set of requirements and that process is under way.

So far we have had positive engagement with not just platforms but civil society and researchers as well on policy in that space. Last year we issued a call for evidence where we asked members of the public and services to provide more information about what exists out there today in ID verification as well as user empowerment tools. I mentioned the two reports that we published over the summer that were really dialling into this area in particular to ensure that we were balancing the information that we got through the call for evidence with the lived experience of people who might have slightly different uses for this—people in politics, sports people, as I mentioned. We are taking all that information now and working through various sets of proposals and we are hoping to consult on those next year.

Q375 **Mr Betts:** Do you expect that to change behaviour?

Jessica Zucker: I expect the category 1 service providers to have to provide those tools to their users.

Q376 **Mr Betts:** Do you expect behaviour to change at the end when you have got this in place?



HOUSE OF COMMONS

This evidence includes content that some may find distressing

Jessica Zucker: Whose behaviour?

Mr Betts: The behaviour of people online and the experience of those who are receiving unacceptable content.

Jessica Zucker: I hope so. Some of my experience has been that putting in additional layers of friction, whether that is through a warning label or having to click through a few more times before you engage or post, tends to be a helpful way to put a bit more of a barrier between people before they post something or they interact with it. The idea behind these user empowerment tools is precisely that, to put a bit more friction between either the person posting something or the person on the receiving end of it. You have a few more options between you and the content that you are interacting with.

Q377 **Mr Betts:** That didn't sound terribly reassuring. I will just draw a parallel with safety in the construction industry, where what you need is a change of culture—that has been identified over the years following Grenfell—with the industry itself and then effective enforcement to deal with the issues that a change of culture does not mean are properly dealt with. Isn't the problem with the platforms that you are dealing with that they are now being subject to different pressures on culture from the United States where anything goes, freedom of speech almost goes above anything else for everyone else's safety and what they are receiving? How do you tackle that? The companies that you are dealing with can't be immune from those pressures across the Atlantic. Is that a major challenge in trying to enforce what you are trying to enforce?

Mark Bunting: I think you have put very succinctly and more clearly the point I was trying to get at earlier that in the end it is as much about the culture inside the companies as it is about the details of the rules. There are those risks. I am not going to pretend that there are not. We have seen changes from industry over the last year or so that have not gone in the direction that we would have hoped, but I think there is a countervailing force, which is the trend globally in the other direction towards promoting user safety and putting that much more centrally in the regulatory environment. We have that in the UK and the European Union but we also work very closely with partners in Australia, South Africa, Canada, Asian and African jurisdictions.

We are starting to see—and age verification is perhaps the best example—a growing global consensus on the importance of changes to protect users, and the US is not immune from that. We have seen individual states in the US bring legislation forward on age verification. That has not been uncontentious but even in Texas there have been laws to introduce age verification for pornography. I think there is more of a consensus on some of these issues than you might expect.

In the areas that are of most concern to this Committee and this inquiry it is true that there is a different perspective in the US on what is acceptable compared to here and in other parts of Europe. We have to be



HOUSE OF COMMONS

This evidence includes content that some may find distressing

really clear in our engagement with the US companies about what we expect, which is compliance with UK law and proper respect for activity that is illegal under UK law, including illegal hate speech. That is a tension that we have to manage, but of course the other thing that we have to be really clear about with industry is that they only have to take the steps to protect users in the UK. We are not trying to restrict the free speech of Americans and we are not trying to ensure that content is taken down globally if it is not illegal in other jurisdictions.

Yes, big picture culture there are pressures, there are areas where there is a great commonality. We have not yet found that the pressures that you have described have got in the way of us ensuring compliance with UK law.

Q378 Samantha Dixon: Talking about compatibility with domestic law, in the Online Safety Act it is an offence to make threats recklessly even if the perpetrator does not intend to carry them out. Meta's policy is to remove threats of violence to public figures only if they are what they describe as "credible". Is that policy that Meta has of only removing threats when they think it is credible compatible with our domestic legislation?

Mark Bunting: I don't want to comment on specific companies' terms, but the key point is that we are absolutely clear that companies' terms of service have to prohibit activity that is illegal under UK law. It would not be good enough for a company to say they have set the bar for threats in a different place to the place that UK law sets it.

Almudena Lara: When it comes to UK users, obviously.

Mark Bunting: When it comes to UK users, exactly.

Q379 Sir Jeremy Wright: I want to return to this issue of algorithmic transparency. You will appreciate from our perspective the original logic for this piece of legislation was suspicion—let us put it no higher than that—that a business model within these companies drives algorithms that promote bad content because it keeps people on the platform longer and keeps them sending more ads. They are using that business model. That matters to us because the more of this bad content there is and the higher the temperature of political debate, the more likely you are to get the content that we are all worried about. The issue of what you can see and how their algorithm works matters, as John was saying.

The bit that interests me is that if I were one of these companies—and two of you have worked for them—that is the bit I would fight hardest about because these are significant technologies. There are huge intellectual property issues here. They will not want to share this technology. I am interested to hear from you your appetite for legal discussion and fight on this question. My expectation—perhaps it is yours, too—is that when you start to use the transparency powers that you have, that is one area where you will find the most pushback from the platforms.



HOUSE OF COMMONS

This evidence includes content that some may find distressing

Can you tell us a bit about your appetite for the fight here? I cannot remember well enough—Jessica will know better than I do—what section 100 actually says, but the word “proportionate” appears in most places in that Act and I suspect it appears there too. Therefore, the argument that their lawyers will make is that it is not proportionate for you to ask us to disclose this because there are all sorts of downsides from our point of view that outweigh the upsides from yours. You do not have to litigate these cases for me now, but just tell me something about your appetite for the fight here.

Mark Bunting: We have already launched a monitoring and evaluation programme that is getting into this area. I have been clear as we have developed our approach to implementing this that we have to have the data from platforms to enable us to assess whether users’ experiences in the end are getting safer. That is not the same as a compliance question because a company may have all the right systems but, for entirely independent reasons, including wider cultural reasons, see an increase in harmful content on its service. Setting the compliance question to one side for a second, I have been clear that we have to gather that data.

We have started that debate already with companies. In particular we are asking for information on the levels of exposure of users to illegal and harmful content in certain categories and how that is changing over time, which is closely related to the question you have asked about algorithms. I will not comment on individual cases here. There has been debate about it, as you can imagine, on proportionality grounds. I am confident where we are now that we will be able to get the information that we have asked for and we feel we have a strong legal basis to do so.

Q380 **Sir Jeremy Wright:** You are prepared to litigate the issue if it comes to it?

Mark Bunting: Yes.

Sir Jeremy Wright: The first of those cases, as we all know, will be significant for setting the tone.

Jessica Zucker: If I could also jump in here, I have a few other points and one learning from the video sharing platform regulation regime, where we did test out our transparency powers. My experience from running that regime was that we got pushback on some of the questions that we asked platforms that we wanted to publish, but perhaps not how I expected. It tended to be more because there was a concern about a perception of comparing apples to oranges. You cannot ask one platform for their metrics on content removals and then try to compare that to a totally different platform. That is a fair challenge and we wanted to think carefully about that. That said, I expect that the concerns that you raise will probably be facing that once we have our transparency reporting regime up.

Q381 **Sir Jeremy Wright:** Presumably, there is a distinction between the



HOUSE OF COMMONS

This evidence includes content that some may find distressing

material that you want to see as regulators and the material that the platform publish. Most of the IP issues apply to publication, not to what you as regulators can see.

Jessica Zucker: Yes, exactly.

Chair: There has to be commonality across what is put on the platforms.

Jessica Zucker: Yes, in some ways. With this distinction of information for regulators and information for the public, you are right that proportionality has to be at the heart of this. One way that we are thinking about proportionality in this is we will ask all categorised services the same set of core questions that we will then use to measure year on year. Each year we will also, in addition to that, choose a thematic area of focus. That thematic area of focus may be more relevant for some categorised services than it will be for others, and that is one place that we will consider proportionality.

Another way that we may be able to consider this is through using risk assessment. Where we see that there is a high risk for whatever thematic area we are focusing on that year, we will have much more leeway to think about proportionality differently for those services and the questions that we may ask.

The last thing worth mentioning when it comes to general transparency around algorithms and information to the public is that there is a real opportunity here for the Government's future researcher access to data regime, which they are thinking about. UK researchers do not have the same access as EU researchers do. That will make a huge difference to being able to level the playing field and make the sophisticated researcher environment in the UK able to take a look at the information in these reports.

Q382 Sir Jeremy Wright: Yes, I completely agree with that. I have one other thing, if I am not hogging it too much. The question of proportionality, as you say, is fundamental here. Is it Ofcom's view that the right way to look at proportionality here is to balance the downsides for the platform in the disclosure of this data with the upsides of safety for the user base? In other words, are you prepared to argue the point that even if there is damage to the commercial interests of a platform in the disclosure of how an algorithm works, if you conclude that that algorithm is doing enough harm to users of the platform, you would be prepared to say, "We still think it is proportionate to ask you for it"? Is that the right way to look at proportionality, in your view?

Jessica Zucker: It is hard to say in an absence of looking at specific examples of that. This will come down to specific arguments, but the broad sentiment that you have laid out is essentially how we will approach it in thinking about risk to users and the opportunity, but we will evaluate and scrutinise any pushback based on commercially sensitive information. There may be other ways for us to think about it.



HOUSE OF COMMONS

This evidence includes content that some may find distressing

Rather than asking for specific quantitative metrics or specific descriptions about a system and risking bad actors gaming that information when you put it out, we may be able to take a different approach and ask for an illustrative case study or something like that. We are keen to try—

Sir Jeremy Wright: Or to disclose it to you without it needing to be public information.

Jessica Zucker: Exactly, yes.

Mark Bunting: Yes, I completely agree. I would probably frame it slightly differently from balance. The proportionality question for me—and the response to a challenge—is being able to demonstrate that we have taken the most efficient and cost-effective route to achieve our statutory objectives. That may still be expensive or problematic for the companies, but if that is the most effective way of us doing our job, that is what we have to do.

Q383 Sir Jeremy Wright: The problem is your statutory objectives include the word “proportionate” most of the time. You will have to decide what you think proportionate means to apply that test, which is why I am asking for a sense. I appreciate what Jessica says that they are all context-specific, but as a general approach. Again, we are interested in knowing that you will not simply hear from a platform, as you will, “This is terribly difficult and expensive for us” and then conclude that it cannot be proportionate to ask for it. There have to be other things to consider, like the interests of the platform users.

Mark Bunting: Absolutely.

Almudena Lara: Some of our measures in the illegal harms and the protection of children codes speak to that because there are expensive but necessary things to meet the objective in the Act of protecting users from illegal content or children from harmful content, and we have included those. We would apply a similar logic.

Q384 Chair: On what you were saying about the platforms’ comparatives being completely different, I am saying that commonalities are put on every platform for the same people with the same message. Proportionally, that is there. I worry that you have some who want to behave and follow the codes and others who do not. To me, the same measures should be used. You get tougher with those who are more difficult than those who are in line. What is your strength, Ofcom?

Mark Bunting: The way that I would frame it is having the powers to enforce the rules but also having the resources to engage constructively with firms to secure compliance without having to always take enforcement action. Some regulatory regimes are much more legalistic in their nature and are much more oriented around the bringing of cases. Sometimes that is appropriate, but if you always have to go through a legal enforcement route, it is costly and time-consuming, and often the



HOUSE OF COMMONS

This evidence includes content that some may find distressing

problem has gone away by the time a judge has decided that you have done the right thing.

We have tried in building this regime to invest heavily in teams that can build relationships with industry. We will not always be able to secure compliance voluntarily but, where we can, we will. We think that is a more efficient way of securing the change that Parliament wants.

Q385 **Chair:** What is your weakness?

Mark Bunting: It is not our weakness, if I can put it that way.

Chair: If there were a weakness, where would it be?

Mark Bunting: The challenge is the scale of the task. It is the diversity and number of companies in scope of this regulation and the wide range of issues that Parliament has asked us to tackle. We have talked quite a lot today about important issues of great concern to people, which we do not have the powers to tackle. Even the job that we have is broad. We are conscious of the need to be able to demonstrate that we are making progress and securing improvements for users, even though we are also conscious that will not solve all the problems that people quite understandably worry about.

Q386 **Chair:** How will you measure success?

Mark Bunting: We will measure success by meeting the objectives that we have set out. I talked at the beginning about the areas that we are looking for immediate improvement on.

The first step for us will be about whether we can demonstrate that companies have adopted the safety systems that we have required. That itself will take time, but we will publish our initial report later this year on the changes that we have seen in the first year of the legislation being in force. The second part of it is the discussion we were having about what that means for the users of these platforms. Can we show that people are less likely to be exposed to illegal and harmful content online over time compared to where they are now? That is the long-term measure of success.

Chair: And failure?

Mark Bunting: Failure will be if we do not achieve those things and if we do not succeed in seeing the change in industry that we have had a good discussion of today, including the cultural points as well as the use of the measures that we have recommended.

Q387 **Chair:** If one measure would make the difference, what would that be? If we could grant you one thing, what would that be?

Mark Bunting: For change in the industry?

Chair: Just to be effective and deliver what we are expecting.



HOUSE OF COMMONS

This evidence includes content that some may find distressing

Mark Bunting: The biggest change would be a commitment at the highest level to the companies that we are regulating to implement a more comprehensive approach to risk management of the kind that we have set out. That is the change that I would recommend.

Q388 **Chair:** Everyone will turn around and say, "Another toothless tiger. Here we go again." How do we make sure that that will not be the case? I am giving you the opportunity to say. What will give you the teeth that you will need to make sure that we can see that you can bite?

Mark Bunting: We are six months into the implementation of this regime. We are confident that we have powers that will drive the change that parliamentarians are seeing. We will not be able to address all the issues that we have discussed today.

Q389 **Chair:** Are these milk teeth rather than real teeth if you are only six months in?

Mark Bunting: A good analogy. They are real teeth, but they are not necessarily sharpened in all areas yet.

Chair: All right. Can I say thank you if there is no more questions? Sorry. Please, John.

Q390 **John Slinger:** Building on what Mr Speaker said, you have been criticised by people in the United States. You and us collectively as a country, and probably a Government and a Parliament maybe, are likely to come under more attacks around freedom of speech and overly zealous regulation, as they would see it. I noticed that Lord Grade, your Chair, gave a good speech in July where he outlined a robust defence of freedom of speech. This is not about freedom of speech, in my view. This is about decent behaviour online as it is offline. Do you feel that you, as an institution, have the firepower to defend yourself against what might become an amplified, sustained attack on the work you are about to do more of?

Mark Bunting: Great question. We are clear on the job that we have been given to do. We cannot be deterred from that job by pressure from other jurisdictions. It makes a tremendous difference to us to know that we have the continued full-throated support of parliamentarians and Government in doing the job that Parliament has given us. We very much appreciate that support. There is a widespread consensus in Parliament about the importance of this job and that has been reflected in the discussion we have had here. The more we can rely on the support of parliamentarians, the more comfortable we will feel.

Chair: I am afraid we must end it here. Thank you for speaking to us today. If you did not have the opportunity to say something or if you have further thoughts that you wish to share, please send them in writing to the secretary. I would be grateful if we could clear the room. Thank you for turning up. We appreciate it.