

Science, Innovation and Technology Committee

Oral evidence: Work of Ofcom, HC 918

Tuesday 20 May 2025

Ordered by the House of Commons to be published on 20 May 2025.

[Watch the meeting](#)

Members present: Chi Onwurah (Chair); Emily Darlington; Kit Malthouse; Dr Lauren Sullivan; Adam Thompson; Martin Wrigley.

Questions 1 - 123

Witnesses

I: Dame Melanie Dawes, Chief Executive, Ofcom; and Natalie Black, Director, Communications and Networks, Ofcom.

Examination of witnesses

Witnesses: Dame Melanie Dawes and Natalie Black.

Q1 Chair: Welcome to this one-off session of the Select Committee for Science, Innovation and Technology on the work of Ofcom. We have heard from Ofcom recently as part of our inquiry into social media and harmful algorithms.

Today, we are very pleased to welcome representatives of Ofcom, Dame Melanie Dawes and Natalie Black. I will ask you to introduce yourselves when you speak. I start with my declaration of interest: I worked for Ofcom, almost from its inception in 2003 until my election in 2010.

The first chair of Ofcom, Lord David Currie, made it explicitly clear that he did not want Ofcom to be involved in the regulation of the internet; he said it was too controversial and too complex. Of course, the Online Safety Act is how the UK regulates the internet, so I am particularly interested to know how its implementation is going so far.

Dame Melanie Dawes: Thank you very much, Chair. I am Melanie Dawes, the chief executive of Ofcom. Thank you for inviting us today.

You have the benefit of knowing those early years of Ofcom's history, which I do not. Back in the 2000s, and even right into and through the 2010s, I think the idea of regulating social media was not something that was embraced very quickly by any jurisdiction or any Government, and certainly not by regulators who might have been in the frame for it. What we have seen over the last five or 10 years in particular—the acceleration in harm, particularly to children—has led Governments to act. Our own Online Safety Act in the UK, passed at the end of 2023, is one of the most ambitious pieces of legislation in the field globally. In fact, I think it is the most ambitious.

How are we doing so far? Briefly, Parliament gave us 18 months to get finalised the codes on illegal harms and the protection of children, and rules for age verification for pornography providers. We have done that. We met that deadline at the end of April. Some of the rules are in force. We have already started enforcement, where that is the case. By the end of July, when the children's codes become enforceable, that initial piece of work will be concluded. There is still more to do with so-called categorised duties and a few other important policy areas, but we are already up and running on driving compliance through supervision and enforcement. The last few months have been a real turning point for us and I think the industry is starting to feel that as well. They are starting to see us getting real about driving through the changes with all the tools we have at our disposal.

Q2 Chair: Thank you. It is good to hear how you are progressing against the milestones set out. I think what most people would judge the implementation by would be the level of online harms that are being experienced, particularly obviously by children. The Molly Rose



HOUSE OF COMMONS

Foundation—as you know, set up in memory of Molly Rose, who tragically at the age of 14 took her own life—recently said that “no one can credibly claim that Ofcom’s implementation of the Online Safety Act is anything other than a disaster.” How would you respond to that?

Dame Melanie Dawes: We have so much respect for Ian Russell and other parents who have campaigned on this over a number of years. We meet with them very regularly. I meet very regularly with some of the families and other survivors of online harm, and so does my team.

We are always very sad to hear people like Ian saying things like that, but I just do not agree with him on this occasion about the children’s codes that we were announcing on the day that the Molly Rose Foundation said that, at the end of April. I do not agree that they are weak and that they will not make a difference. They represent a huge change in industry practice for protecting children.

We have an enormous task on our hands now to drive compliance with those rules. There is no question about that. That is only starting now. We are very determined to make a difference. You are absolutely right that the proof of what we are doing, and its impact, will be when we see changes in the systems and processes of companies online and, ultimately, people reporting that they have less harm than they did maybe a few years earlier.

Q3 **Chair:** Molly Russell took her own life after seeing content that glorified and encouraged eating disorders. The Committee has heard evidence that that type of content is still online. You talk about enforcement and compliance, but is there content that you think you cannot regulate, or other online harms that you think you cannot regulate, stop or prevent?

Dame Melanie Dawes: Suicide, self-harm material and eating disorder content is harmful for children, even if it is legal for adults. Some of it is illegal, actually. Pro-suicide content, for example, is just plain illegal. Other content may not be, but the Act is very clear, and our codes are very clear, that that is primary priority content and it must not be shown to children under the Online Safety Act. There are measures in our codes that start with the need to have highly effective age verification if you have children on your platform, or you are likely to. If you have that content on your platform, you must have highly effective age verification at age 18 and, secondly, under-18s must then get a different experience from adults. They must not be shown material like that, or violent content, misogyny and so on. It includes pornography as well. Those are the rules.

Can we regulate that content? Yes, I think we can. There are always difficulties for companies in defining the boundaries there, but particularly when it comes to protecting children we expect them to exercise caution. Fundamentally, it is about how their algorithms work. They do not have to take the content down; they just have to not show it to children in their feeds.



HOUSE OF COMMONS

I did not answer your question about what we could not regulate, but I wanted to explain how we can deal with that incredibly important category of content.

Q4 Chair: I appreciate that Ofcom's position is that you can regulate that content, and you will seek enforcement. To my question, are there online harms that you believe you cannot regulate and/or should not regulate?

Dame Melanie Dawes: The Act is clear that it is about illegal harms. There are more than 130 of those listed in the Act, things like child grooming, the exchange of child sexual abuse material—

Chair: I think we are clear that illegal content is regulated.

Dame Melanie Dawes: That is the focus for adults. For children, as I was explaining, there is a broader category of content. What is not covered is so-called legal but harmful material for adults. There was a big debate about that in Parliament, as you know. What is also not covered is the debate that we are increasingly having about the time that children in particular, and adults perhaps, spend online, and addiction and the nature of those algorithms. There are some wider mental health harms that are increasingly a concern to parents, and which I completely get.

I would not say, sitting here as the regulator, that we should not regulate those things. When you get into legal but harmful material, it is quite difficult because of the boundary issues and the need to protect freedom of expression. In the end those broader questions are going to be asked. My job is to get on with making the internet safer. If companies cannot deliver on that, maybe they will face more draconian rules in future.

Q5 Chair: As you say, your job is to get on with making the internet safer, but I think you recognise that there is harmful content, particularly for adults. We have heard how harmful content is accelerated and pushed out through recommender algorithms. It is harmful content that you, currently, do not regulate. I think that is what you are saying.

Dame Melanie Dawes: Yes, there are some categories of legal but harmful content that are not regulated for adults, in particular. That was a decision that Parliament made. It was long debated. There was mis- and disinformation, for example; non-illegal hate speech and so on. Those were not covered by the Act, although, when it comes to violence against women and girls, Ofcom has already published draft guidance that sets out best practice in those areas because they are clearly important.

Q6 Chair: The Minister certainly gave us the impression that her view was that Ofcom could regulate mis- and disinformation, but we will come back to that.

Before I open this up to other members of the Committee, I want to ask Natalie Black a question. Natalie, you were deputy head of the No. 10 policy unit from 2015 to 2018 and director of the internet harms unit



HOUSE OF COMMONS

from 2017 to 2018—the Online Safety Act took a long time to get through Parliament—when discussions about how we can, or should, regulate the internet were taking place under the previous Government. Were you involved in those discussions, and are you now marking your own homework?

Natalie Black: First, good morning. My name is Natalie Black. I am the group director for networks and communications at Ofcom. As you mentioned, Chair, previously I ran the No. 10 policy unit and kicked off the original work around online safety. My role at Ofcom is focused on networks and communication. It is predominantly digital infrastructure, but I also lead our work on AI.

One of the great joys of working at Ofcom is that we are a collaborative team and we work together across a whole range of issues. Certainly, for the companies that we engage with, we regulate whether they are under online safety or, potentially, under some of our digital infrastructure regulation. I hope that explains that I have a specific role, but, of course, I work with colleagues across the board because these are cross-cutting issues.

Q7 Chair: Do you think that the Government should have started the process of regulating online content earlier when you were in No. 10?

Natalie Black: I am not sure that is one I can judge. At the time—nearly 10 years ago now—the world was quite different. Certainly, what was recognised was that increasingly tech companies were having an impact on consumers' lives in a way that probably had not been anticipated. At that stage, the UK was at the fore, as it continues to be today, in trying to tackle some of those very difficult issues.

Q8 Dr Sullivan: I want to ask a little bit about how you are going to drive compliance. In particular, will you be searching for harms or are you going to wait for the harms to be delivered and then reported so that action can be taken? I want to get an idea of how you are driving compliance.

Dame Melanie Dawes: That is a really important question. The answer is a bit of all those things. While we were in the 18-month period of having to develop the codes of practice, we took a conscious decision to invest in supervision teams. There is a team across Ofcom now of around 60 to 70 people, working with about 50 companies that are either the large household names that you would expect or small and risky. We thought we needed to understand them and get under the bonnet of how they work, and build some form of working relationship prior to getting into the enforcement and compliance mode.

Those supervision teams will continue, and that is really important. We cannot do our job unless we have a deep understanding of how, particularly, some of the larger and more complex companies work. That is what that is about. It means that we will be much quicker in understanding the risk assessments that they have all just sent us, to be



able to judge where they are adequate and where they are not, and then to do the same on the measures that they are putting in place. That supervision engagement is important.

We have a triage function in Ofcom, which looks at any intel that comes in. It might be a bit of journalism. It might be a report from a civil society stakeholder. It might be whistleblowing, although we have not had that yet. It could be from any source. We have a process for taking those things and judging whether something is in scope. Is it a problem, can we do anything about it and how do we do anything about it if we think we need to? That is quite new, as you would imagine, because we are just getting into that phase, but it is quite important.

Finally, there is outcome reporting. That is difficult because the industry does not measure safety. That is very important to say; there is no existing framework for judging how you measure harm, particularly how you measure the lived experience of people as opposed to just the number of types of content on a platform, so we are developing a programme of measuring outcomes. A lot of that will be by tracking people's views in surveys. We will measure how systems and processes are being implemented. Things like age verification are quite easy and tangible to measure. With the recommender algorithms it is a bit harder to put your finger on what good looks like, but that is another programme of work that we have in train.

Q9 Dr Sullivan: And anti-religious hate speech or AI-generated images that depict various religions in a negative light is illegal content?

Dame Melanie Dawes: Yes, it can be, if it is racially or religiously aggravated hate speech, and certainly if it is inciting violence.

Dr Sullivan: I will be writing to you on that subject.

Dame Melanie Dawes: Good.

Q10 Chair: You said in response to my questions that Ofcom would be enforcing the guidance in the codes that it has set out. One of the concerns is the way that Ofcom has not provided duties. Under section 49 a provider is "complying with a relevant duty" of the Act if they meet the measures relating to that duty in Ofcom's code of practice, so if you have not set out duties relating to those measures, basically they do not need to do anything. An example of that is with regard to, say, recommender algorithms or misinformation.

Dame Melanie Dawes: There are a few things there. First, harms like misinformation are not named as a harm in the Online Safety Act. That is clear. There are some offences that relate to information that is illegal, such as false communication offences and foreign interference. There are a few specific offences there. In general terms, mis- and disinformation are not harms named under the Online Safety Act. They are not covered by our codes of practice because it is legal content, whereas our focus for



HOUSE OF COMMONS

adults in particular is illegal content. That is just the scope of the overall Act and what it is trying to tackle.

The second thing is the safe harbour nature of the codes, as it is sometimes referred to. Again, in the Act the way it is framed is that companies have to do risk assessments. That is the first thing. If they find something in their risk assessment—we are going to be absolutely scrutinising the risk assessments of the companies we think are, at this stage, either the biggest and the most used or the most risky—and there is not a measure in our codes that tackles that particular risk, we will say to them, “What are you going to do about it?” Just because there is not a measure in our codes does not mean that they can leave a risk in their risk assessment unmitigated

Q11 **Chair:** But they have to identify that risk.

Dame Melanie Dawes: They do.

Chair: If they do not identify that risk—

Dame Melanie Dawes: And we do not manage to find it and challenge it. Bear in mind that this is going to be a very evolving regime. The third thing is—

Q12 **Chair:** Can you identify risks that they do not identify?

Dame Melanie Dawes: Yes. This is where broader monitoring is really important, and all the intel that we will get. The other thing that we will absolutely do is this. If we see that there is a risk that we were not covering off, or a new technology or a new system that can tackle a risk that was not there before, we will adapt our codes. In the next month we are coming out with some new measures that will cover things like livestreaming risks for children; the need for emergency response protocols when you have events such as the riots last summer; the use of automated content moderation; and a few other things. There will be a package where we were not able to get it in the codes the first time around, for whatever reason, but we are moving pretty fast to bring it forward now.

Q13 **Emily Darlington:** There is a broad question that we have struggled with in the Committee. Do you think there are the same rules for online and offline content, and does the Online Safety Act regularise that?

Dame Melanie Dawes: Largely, yes, but if I was sitting here with my experts, they would immediately start to say, “Well, it does depend a little bit.” Largely, the Online Safety Act says that if it is illegal content offline, it is also illegal online and therefore companies need to have systems and processes in place to tackle it. There are a few exceptions, I think, but that is broadly what it is trying to achieve.

Q14 **Emily Darlington:** I think one of the exceptions that you might be talking about is violent porn.



HOUSE OF COMMONS

Dame Melanie Dawes: Do you know, that is exactly what I was thinking about.

Q15 **Emily Darlington:** Very clearly, there is stuff that is illegal to show in a movie theatre or, when we used to have Blockbuster Video, would be illegal to rent and illegal for publishing platforms—Netflix and the like—to do because they do not meet our standards set by the British film council. If they do not have a proper rating, they are deemed illegal.

Dame Melanie Dawes: Yes. There are some categories of pornography that are not illegal online when they are illegal offline.

Q16 **Emily Darlington:** Exactly. When we say offline, some of that still is online in regulated areas and some of it is not, social media being the area that is not. Do you think there is a gap?

Dame Melanie Dawes: We worked quite closely with Baroness Bertin on her review of these issues. She has done a really amazing piece of work. It is very difficult work to do.

There are a couple of things. The Online Safety Act requires all the illegal content duties of pornography providers that are user to user—in other words, ones that allow so-called creators to be on their platforms and have a direct user-to-user business model. That is increasingly the way that the industry is moving. What that means is that those services are, in the language of the Act, so-called part 3, and the full weight of the children's code and the illegal harms codes therefore applies to them. That means that illegal content of many types—I would have to check exactly what the situation is around offline illegal porn—is caught. We have some purchase on some of the issues when we are talking about those kinds of platforms.

Where it is the more traditional, old-style publisher model of porn—the so-called part 5 of the Act platforms—the only requirement on them is age verification at age 18, which we are making good progress on. Keep children out of all of it, is what the Act says.

Q17 **Emily Darlington:** Even if it is content that is illegal offline. That is where we struggle with some of the stuff—how that works. It is not necessarily about creating more illegal content; it is just about regularising the position.

We heard very clearly from the online platforms. They were asked very directly in our inquiry around misinformation in the riots whether they would do anything different now that the Online Safety Act was in place. They very clearly said no, they would not have done anything differently. Is that your read of the Online Safety Act? Is that a problem with the Act, or is it a problem with their interpretation of the Act?

Dame Melanie Dawes: We do not agree with them on that. In fact, we sent a letter to the Secretary of State, Peter Kyle, last autumn reporting on what we had learned from the terrible events of last summer and what



happened online. We are very clear that illegal content was allowed to circulate that showed that the right systems and processes were not in place to tackle it.

Companies that had emergency response protocols, and activated them, did a much better job and worked quite closely with the Government and law enforcement agencies, which is the other thing that we would expect to see in circumstances like those. We are coming forward with a new measure—an emergency response protocol measure—in the package of extra measures that I mentioned earlier, but we have already said in public that we think there were quite a lot of things that the industry would have needed to do differently. Some did much better than others. Those that saw what was happening, activated their systems and engaged with the Government did a good job. It is never perfection in a time like that because things move very fast, but some did not do so well.

Q18 Emily Darlington: Finally, I want to raise the issue of transparency, in particular the challenge around transparency for large versus small platforms, and how reliant the Online Safety Act is on their own transparency. Do you think we have the balance right in terms of their more public or research-based transparency so that we can hold them to account in their own homework marking? Do you think we have the balance right between the large and the small platforms? Given that this is such a big issue for your own road map, do you find any challenges in meeting the deadlines that have been set in the road map because of lack of transparency or a focus on very big, well-known platforms versus some of the more harmful, smaller platforms that go undetected, but where we know a lot of illegal activity is shared and created?

Dame Melanie Dawes: We believe that transparency is a very important regulatory tool. I think, although we will have to see, it will be most effective from the larger companies that have a brand and are widely used by the public. That is where the transparency rules will be tightest. For the categorised services, essentially the larger ones—not entirely but largely—we will be able to issue transparency notices requiring them to publish reports on whatever topics we have chosen. We are going to do that as quickly as we can once we have been able to finalise the categorised service register.

The transparency requirements on smaller platforms are not as great as they are for the big ones. There, what we have already done is open four enforcement investigations—going straight to enforcement, to be honest—where we have seen small but risky platforms that have illegal content, in the case of the suicide forum into which we opened an investigation in April, and two porn sites and a nudify app in the last fortnight. We are going straight to enforcement; we are just not getting any engagement at all and we have a serious concern that there is a high risk to the public.



There will be different tools for different companies. Transparency is important. Should we have more requirements on smaller companies? At this stage I would not say that was the priority, but our whole philosophy on this as Ofcom is that we will learn a lot over the next few years. If we think that there are things we could do more of, and we need more powers to do them, we will talk to the Government about that. I think they are in that learning mode as well, to be honest.

Q19 Emily Darlington: To follow up on that specific point before passing over to colleagues, you said that in transparency reports where they identify risk, you can also identify risk, so it is not just self-identified. How are you, or researchers in universities, going to identify those risks if there isn't the transparency on the data to be able to identify risk? It limits credible flag raising from other organisations, does it not?

Dame Melanie Dawes: Yes, I think it does. You are touching on a very important point. We support any measure that allows researchers and external organisations to go in and interrogate what is happening online. I hope I conveyed earlier that, from Ofcom's perspective, we want a completely open door for any information that people are able to bring us. What we get from our regulatory relationships will be one side of the story. A lot of it will be information that no one else has access to because it is commercially privileged. Researchers are often in a brilliant place to be able to do truly interesting research, but at the moment they cannot always get access. In fact, they usually cannot get access to the data that they need. I think that is very important.

Q20 Martin Wrigley: I previously worked for the Phone-paid Services Authority, which is now merged into Ofcom. I no longer do that.

I sat on the Committee for the statutory instrument that looked at the categorisation of services. We were somewhat perplexed, and I still do not understand from your answers so far, why you chose not to enable the hard-won modification to the Online Safety Bill that allowed you to put into the most restrictive categories or the most regulated categories those small but harmful services. In your recommendations back to the Government as to what you wanted in that SI, you deliberately excluded that. That perplexed us all, and it still perplexes me. Why did you do that?

Dame Melanie Dawes: There are two reasons. First, we do not think that that part of the Act gave us the flexibility to add risk that would have allowed you to go after smaller and risky sites in the categorisation framework. We did not believe that we had that discretion.

It is long debated. I was going through it last week, line by line, with our lawyers. We were reminding ourselves of exactly where we were. I do not have the document in front of me, but fundamentally it is framed around reach. That is essentially the driving principle behind that bit of the Act. We did not feel that adding risk that was not associated with reach was in tune with that part of the Act. I know there is a lot of debate about that,



but it is just not something that we felt was part of what we were able to do.

If you look at the duties on categorised services, in our opinion they are not very well targeted at the risks of small but risky platforms. What we have done in our codes of practice is to be very clear that the most stringent measures against illegal harms and for the protection of children apply to small but risky platforms as well as large but risky platforms. At Ofcom, we genuinely believe that the statutory codes of practice give us what we need to take action against small but risky platforms. We are already taking action. As I was saying, we have taken out four enforcement investigations in only the last few weeks. We have three further programmes looking across the whole industry at small but risky companies, as well as some big ones. It is on the basis of the evidence we have about what we think we are able to do, but also our legal reading of that part of the Act. We are very happy to follow it up. It almost requires you to go through it line by line, but we are very happy to take that offline, if it is helpful.

Martin Wrigley: Yes, please.

Q21 Adam Thompson: Good morning, both. Thank you for joining us. I want to pick up on some of the points that you and Emily were making a few minutes ago, looking at transparency. I think you had a really good discussion there about transparency of the companies that you engage with, but transparency works both ways, of course. Do you think that Ofcom should have a duty of transparency, particularly regarding the meetings that you have with companies you are engaging with? I mean the big tech firms. Obviously, you have to have those meetings, but do you think there is a duty of transparency to talk about them?

Dame Melanie Dawes: We are required to produce transparency reports, which is not what you are talking about but, just to be clear, there are some transparency duties on Ofcom as well in terms of our reporting. On the question of transparency about the meetings we have, I do not think you will find a regulator that routinely reveals the details of the companies that it is meeting because of the need to preserve commercial confidentiality. That is part of it. Even just giving the names and the meetings risks having a chilling effect on those discussions.

We thought about it long and hard, and I completely understand the challenge. It is a very fair one. We are subject to freedom of information, of course, so there are times when, if we are asked for specific information, that will be caught by the FOI Act. I do not think you will find regulators that are comfortable releasing information on who they talk to. As I say, it can reveal, for example, that you are very concerned about a risk and that you are talking to a company about it. That may simply not be something that is helpful to progress in an investigation at that particular point in time. That is where we are on that issue.

Q22 Adam Thompson: I take that point. I think it is moderately concerning,



HOUSE OF COMMONS

but I take what you are saying. In a recent letter to the Committee, Ofcom said that you are developing a range of ways of updating stakeholders on these meetings. Can you elaborate a little more on what that update process looks like, and what you think it should look like in the future?

Dame Melanie Dawes: We are publishing a regular bulletin on supervision and enforcement. That will be one of the primary ways that we are able to say, certainly using numbers, how many companies we are meeting, how many we are supervising and so on. Of course, the moment we open an enforcement investigation we are absolutely clear about the name of the company that we are enforcing against unless, as in the case of the suicide forum, we think it is helpful to them to give their name, which we did not want to do. No one names that forum in the press or the media. The supervision and enforcement bulletin will be the main way that we keep people updated.

Q23 **Chair:** An enforcement bulletin does not give transparency about who you are engaging with. When I worked for Ofcom I remember there was so much more pressure to meet big companies like BT than small companies, which often do not have the time. How can we understand the extent to which you are engaging with big tech rather than small and medium-sized businesses and, particularly, citizen representations? My constituents have the impression that big tech is all in league with Government, and you are kind of playing to that if you say you are not willing to share how you engage with companies.

Dame Melanie Dawes: Natalie might want to say something about this, because she leads all our engagement, with me, on the telecoms side for example. I am just giving you my honest answer as to why we think this could stop us being able to do our job effectively. That is why we have taken—

Q24 **Chair:** Could you, for example, share how many hours you spend per week with companies of over £100 million in revenue, versus companies below that? If we accept the commercial argument, which I am not sure I entirely do, there are still ways around it to demonstrate how you engage with a range of companies.

Dame Melanie Dawes: We are certainly very keen to explain our overall approach and what we do. We absolutely do engage extensively with civil society.

Q25 **Chair:** But you are not willing to put any kind of volume on that. Is that something you can look at and write back to the Committee?

Dame Melanie Dawes: We can certainly look at how we might improve on it, but I do not think we will change our view that giving names of companies is potentially quite risky for us to be able to do our job. Natalie, do you want to give a perspective on that?



Natalie Black: Let me give two examples that might highlight where some of the challenges are. On the telecoms access review that we are running at the moment, we will receive a wide range of consultation responses. Those are made publicly available. That is a lot of data that we put into the public domain. An area that is more challenging is cyber-security. Companies come to us to let us know that they are experiencing breaches. If there is a chilling effect, as Melanie mentions, it can increase their reluctance to come to us, which can increase the risk for the overall sector, but particularly if it is live—there are obviously a number of live cyber-security events in the UK economy at the moment—there are real implications for how the threat can increase as a consequence of what information is in the public domain.

In terms of holding us to account, we are required under the Telecommunications (Security) Act 2021 to write to the Secretary of State and provide a report on progress and where there are incidents. I use that as an example to highlight that there are levers. We take those responsibilities very seriously, but, as Melanie says, we can consider where else it might be possible to increase the volume of data.

Q26 **Chair:** It is really important that you hear the voices of businesses of all sizes—

Natalie Black: I agree.

Chair: And consumer and citizen groups. For the moment I do not see any way of measuring how you are doing that, and how it evolves. But you will write to us and set out how you will take on that challenge.

Natalie Black: Maybe I could add this, not to draw out the point, but to emphasise that I very much agree with you, because when we talk about Ofcom's responsibility for consumers, the definition of consumers is very wide, and SMEs in particular are significant consumers in the economy. We spend time with the Federation of Small Businesses and the British Chambers of Commerce, for example, and Citizens Advice. It is a question I asked my own management team: "Who are you spending time with?"

Q27 **Chair:** Let us share some of the answers.

Natalie Black: I want to emphasise, though, that that is something we take very seriously—the broad definition of consumers.

Q28 **Dr Sullivan:** The question is always: "Who guards the guards?" Who are the people who can see and check on the judgments that you are making, to ensure that transparency? At the minute, it feels like a closed book, and we are here to trust you, which we can do, but how do we get that assurance? If you can write to us with where those levers are—you mentioned the Secretary of State; if that is the only lever by which to see what is happening—

Natalie Black: That is one example.



Dr Sullivan: If you could expand on the others, that would be great.

Dame Melanie Dawes: We get the challenge, and are very happy to take it away and see how we can really improve on this. Fundamentally, we are an independent regulator and we are accountable to Parliament.

Chair: Through sessions like this.

Dame Melanie Dawes: This is one of the main mechanisms of accountability, right now, and we take that very seriously. We are also accountable through the courts for our individual decisions on the companies we regulate, but fundamentally we are trying, on online safety, to be as transparent as we possibly can be. We publish so much research and information about what we are doing, but I will take away this particular question and see how we can at least give you a much clearer picture of who we are meeting, what our approach is, and some detail behind that.

Chair: Okay, that is great.

Q29 **Adam Thompson:** We discussed mis- and disinformation a bit earlier, but I want to pull in a few points about that broad theme. In particular, the Online Safety Act requires Ofcom to set up an advisory committee on mis- and disinformation, but we recently heard that the words “misinformation” and “disinformation” had been removed from the name of the committee. Can you explain why?

Dame Melanie Dawes: We were able to start setting up the committee when we had a non-executive member of our board with the relevant experience of online services and mis- and disinformation, in Richard Allan. He was appointed last autumn and moved pretty sharpish to set up the committee and get it going within four or five months. It is now up and running. It had its first meeting on Friday. From his knowledge, during the process of recruiting people for the committee, he concluded, and persuaded the board, that there is a broader use of language going on around information. People talk about “information disorder”—I think that is a phrase that Full Fact used, for example—“healthy information systems” and so on.

We consciously decided on what we think is a slightly broader name. Clearly, though, there is no question but that it covers mis- and disinformation: false information that is misleading and harmful because there are public health implications or simply because news and current affairs are being degraded, or because of fraud, which is very related to mis- and disinfo. We are absolutely doing what the Act requires us to do, but we think this name will stand the test of time a bit better.

You will be hearing from the committee quite soon, because, although they have to produce a report within 18 months of being set up, they are going to look at individual projects and publish those as soon as they can. They will choose topics, so they can get moving quickly. I hope that will



HOUSE OF COMMONS

allay some of the concerns about whether we care about this. We do, but we are just trying to set it up in a way that we think will be effective.

Q30 Adam Thompson: It is safe to assume that, despite the change, the focus on mis- and disinformation is still very much the committee's primary function.

Dame Melanie Dawes: Yes, it is.

Q31 Adam Thompson: On a related question, when we spoke to Mark Bunting he indicated that one reason the name was changed was to avoid having to use the words "misinformation" and "disinformation" over and over again. How much did that aspect factor in the decision?

Dame Melanie Dawes: For us, it is all part of the same point. Something that is a bit simpler—the information advisory committee—will stand the test of time better. Mis- and disinformation are specific parts of that, and probably very large parts of what we are talking about, but there is a slightly broader conversation.

Q32 Adam Thompson: Fine. On the timeline, so we can understand a bit better, I think the Government's statement of strategic priorities for online safety referred to the committee by its original name, supposedly more than a week after the change was announced. Was that just an oversight, or was the decision made at different points? What happened there?

Dame Melanie Dawes: I suspect that was just an oversight. The name in the Act remains, of course. Its statutory name and functions are there in the legislation; it is just the working name that we have given it.

Q33 Adam Thompson: Finally, to clarify, was this name change discussion held internally only, or was it in full discussion with, and with the support of, the Government?

Dame Melanie Dawes: It was a decision by our board, but we discussed it with the Government. That is why I think it was probably just an oversight that the language was not changed in their statement of strategic priorities.

Adam Thompson: Thank you both.

Q34 Kit Malthouse: Dame Melanie and I worked together when she was permanent secretary at MHCLG and I was the Housing Minister. One of the issues that we faced there was the number of good planning officers who were getting poached and moving to the industry. There was a lot of frustration with Ofcom among parents and groups outside about a sense of complacency. I have to be blunt with you: the last appearance we had from Ofcom and the ICO came across to a number of us as completely complacent in addressing what we face together. Exploring the theme of transparency, what does the movement look like between Ofcom and the industry and vice versa? Are you a nice career-development process for future tech execs, and how many have moved from the industry into



Ofcom at senior levels?

Dame Melanie Dawes: It is quite a small number of people who go in either direction, to be honest. Two of our directors in online safety have worked in the industry, and that is hugely helpful because they bring real-life experience of how decisions are taken in those companies. In both cases they have come because they care about trust and safety, as it is known in the industry, and want to be part of making a difference and driving changes that they were not able to drive when they were on the other side of the fence.

We have a few more junior people who sometimes go to the industry, yes. Our staff are going to be attracted. That happens on the telecoms side, as well, and on media. I view that as part of people building a career in expert areas, but our board is really clear about conflicts of interest, for example, and making sure that there is proper gardening leave and the right sorts of firebreaks, if you like, particularly when senior people—

Q35 **Kit Malthouse:** How are you handling those accusations of regulatory capture internally?

Dame Melanie Dawes: By doing the job. I am very sorry to hear that you thought we were complacent last time round, but we are absolutely not complacent. We have a very big and challenging job to do. It is an incredibly ambitious Act, rightly so, and—

Kit Malthouse: I know; I understand, and you have said that already.

Dame Melanie Dawes: We really are not complacent.

Q36 **Kit Malthouse:** Sorry to interrupt. Do you have internal conflict mechanisms? For example, if I am a former Google executive, I cannot work on Google.

Dame Melanie Dawes: Yes, that is correct—for a period of time.

Q37 **Kit Malthouse:** How long is that period of time?

Dame Melanie Dawes: I can send you the details of our conflict guidance, which, as I say, is overseen by the board. It depends on people's level in the organisation, but also on the nature of the work. The decisions that we are taking about enforcement, which are the most important of all, are taken with incredibly clear governance. I am not part of that decision making, for example. It is the same on broadcasting content oversight. It is the same when we are deciding what to do about Royal Mail's performance each year. Those decisions on enforcement are taken with incredibly tight governance, and that is a very important part of it, so that we can be clear that where the most important decisions are taken they are properly objective.

Q38 **Kit Malthouse:** What is the flow of executives like in the other direction—people leaving you to join the firms that they were previously



regulating?

Dame Melanie Dawes: It is unusual at senior levels, but more common at more junior level. People will often be going to trust and safety teams, so they will be going to implement the Online Safety Act in their companies. As you can imagine, that is something that companies are often quite keen on.

I think we have to accept some risk. We worked in the Housing Ministry together. If you have a Government Department—Departments often struggle with this—with absolutely no knowledge of what it is like commercially to be in those industries, you are flying blind. You cannot do your job properly. That is even more important for a regulator, because we have to have a detailed understanding of the companies we regulate, in a different way even from a Government Department. I think you have to accept that there are risks that have to be managed. We are confident that we manage them as well as we can, but we simply could not do our job if we were not able to bring in people from outside.

Q39 **Kit Malthouse:** I understand that, and I accept the need to balance risk. I have just become concerned, quite recently, about general regulatory capture across all our regulators. For me, the biggest one is a former Amazon executive becoming chairman of the Competition and Markets Authority. Here is one of the most anti-competitive firms in the world, and that is my concern.

Obviously, you are not in every meeting. I would be concerned if there was not quite a long period before a Google executive who joined you could have conversations with Google or one of those other firms about their regulatory status, or whatever. You are in a very difficult area. I understand the risk; but there is also a lot of money at stake, and we know that these firms spend a lot of money on regulatory capture, not just here but around the world. They do as much managing of you as managing the market, because they are so dominant. They do not have to worry about competition. That, I think, is where, from a lot of people's point of view, more transparency would be welcome. Would it be possible for you, for example, obviously anonymised, to write to us about the flow backwards and forwards over the last, say, four or five years?

Dame Melanie Dawes: Yes, we can do that. I would also like to paint the part of the picture that is about civil society. In online safety I believe that more people have come in from the NSPCC, 5Rights, the Internet Watch Foundation, the National Crime Agency and other regulators than from the industry.

Q40 **Kit Malthouse:** That is fine. If you are able to show us the numbers in both directions, that would be helpful.

Dame Melanie Dawes: We can certainly have a look at that.

Q41 **Kit Malthouse:** As a small part of your conflict declarations, do staff have to declare if they are approached by a recruiter or a firm with a



possible offer of employment?

Dame Melanie Dawes: At a senior level, yes. We have rules on that.

Q42 **Kit Malthouse:** At any level?

Dame Melanie Dawes: We do not have rules for every member of our staff, no, but if you are moving to a job where there is a conflict, and if it is a very acute conflict, even if you are quite junior, immediate gardening leave is likely to be required. At a senior level, any member of my team who is approached by a headhunter about a job in our industries is expected by our board to notify me and my general counsel straightaway.

Q43 **Kit Malthouse:** Are you able to give us the numbers of notifications you have had over, say, the last three or four years, specifically of approaches to recruit?

Dame Melanie Dawes: Of the senior ones, the number is one, I can tell you, in the time that I have been at Ofcom, out of my entire senior team. That person did not apply for the job, either.

Q44 **Kit Malthouse:** Just one declaration.

Dame Melanie Dawes: Yes, and there have not been any others. I am confident of that.

Q45 **Kit Malthouse:** Okay, fine. If you could send us that information on the flow backwards and forwards, it would be very helpful.

The second thing I want to ask you is about the attitude you get from the firms that you are dealing with. One of the impressions that I have been left with in my interaction with them, not just on mis- and disinformation but on child safety generally, is that they try to do the absolute bare minimum they can for compliance. They feel no wider duty than that, and even then they wriggle and squirm, and often what they say is not the reality of experience on the platform. Is that your impression in your interactions with them as well?

Dame Melanie Dawes: We are just at the point of being able to start to judge that. We have got all the illegal harms risk assessments from the industry in. We asked for those two weeks after the statutory deadline. They all came in pretty much on time by the end of March. We are interrogating those now. I am sure we are going to see some wriggling and squirming, yes, but it is our job to call that out and sit down and talk about it, and ask for a different risk assessment and, as we start to look at the measures they are introducing, push harder for the measures that we expect. We are going to have to make judgment calls at some point about where to escalate some of those conversations. As I say, we have already gone into enforcement action with some small but risky platforms where we have had no engagement at all. I agree with you; there will be some in the industry who will want to do the bare minimum, or even less, and wait for us to come and find them.

Q46 **Kit Malthouse:** This leads me to the second question about that. The



HOUSE OF COMMONS

other impression I get is that they are actually technically capable of far more than they let on. Take Facebook, for example. You and I both know that the vast majority of child abuse notifications in the UK come through Facebook. They emanate on that platform. Given that they are able to detect that I might need a new lawnmower, and send those adverts to me, or given, for example, that another Meta platform, Instagram, is able to detect and remove nudity automatically, it is perfectly possible for Facebook to engineer their system to get rid of the stuff completely. Do you feel that they are hiding behind complexity in the law and ignoring their capability and wider duty to society to get away with the bare minimum?

Dame Melanie Dawes: I think you are right that the capability is often there, and is being used for different purposes. For example, there is a lot of information on which users are likely to be under the age of 18, from tracking how people use services and so on, but that is not being used to call out that somebody has said they are 18 and is actually only 13, even though the company knows full well that they are very likely to be under age. That is one example. There are many others where the technology is there but is not being used for safety. That is the change we have to drive.

This is a cultural change, above all else. I think that the business models are going to have to change. Some revenues that were being earned will not be earned. Children will not be marketed to in the same way as before, because we will know where they are. The algorithms will not be as viral for them as in the past, so they will not spend as long on the platform, hopefully. That is the change we are going to drive. Some of it will stick and be difficult to force through.

More broadly, maybe you have to be an optimist to work in online safety at Ofcom. I think the industry sees that things are changing. The point of regulation is that we are creating a new standard for everyone. A lot of the companies say to me in meetings, "Are you doing this for everyone?", and our answer is yes. That is very important. It is simply having the benchmarks; something like age verification that you are aged 18 has been nowhere until now, but is slowly becoming the norm. It is our job to push those cultural changes through.

Q47 **Kit Malthouse:** I certainly hope so. With the people I interact with, the experience is that what they say and what they do are two very different things. They hide behind the fact that it is a great big amorphous organisation, so they cannot possibly control every single thing, and things leak through, and all the rest of it, whereas when it comes to their revenue nothing leaks or gets through for free. There is a sort of conflict there.

I want to ask you a final two things. We had a conversation about meetings, and you publicising them. I think it is a kind of proxy for there being some kind of certification, or a sense for people about what kind of platform they are dealing with. Every parent has a sense in their own



HOUSE OF COMMONS

mind, from talking to other parents and kids, and from experience, of which ones are sort of okay and which are awful. Certainly, in my parent group, Snapchat is deemed to be the worst by far, and some of the others less worse—none of them is great.

As you go through the process of regulation, will we have a sense that we are able to judge levels of compliance, as users, particularly those of us who are looking after teenagers? Will it be like the British Board of Film Classification? Will you be able to say, "This platform is safe; this one is not safe"? That is broadly where I think we all want to reach. That is not just about children. It is about misinformation and disinformation. Some of them may have internally recognised it. You have community notes on X and all that, which is a bit dodgy anyway. Really, I think what people want from a regulator is certification that says, "Safe/Not safe." Will we get that?

Dame Melanie Dawes: That binary "Safe/Not safe" certification is not part of the framework of the Act, but what definitely is, and what we will do, is transparency reporting from Ofcom. We have to do that annually. That is where I want us to say very clearly—particularly, I think, for parents—about the household name platforms that we all know children are on: "Here is where they are in delivering on their safety duties." That sense of being able to explain to the public what is and is not happening is very important for us to be able to—

Q48 **Kit Malthouse:** So "Compliant/non-compliant."

Dame Melanie Dawes: Yes, and I do not think it will be binary, because I think our experience is going to be that it will be safe in some areas and not doing enough in others. That is likely to be what we see.

Q49 **Kit Malthouse:** That is non-compliant.

Dame Melanie Dawes: Yes, it is non-compliant.

Q50 **Kit Malthouse:** We saw a couple of months ago a big fuss about Roblox and young people being exposed to quite serious harms. Video games have an age classification. We are obviously moving to age verification, but even within that the 13 to 18 period is still a vulnerable time for young people. Sorry, Dame Melanie, but a slightly vague, "Well, they're all right in some bits but not in other bits," does not allow me as a consumer to judge.

Dame Melanie Dawes: It will not work if it is vague, so it has to be clear.

Q51 **Kit Malthouse:** Okay. The last thing I want to ask you about is the rise of the use of VPNs and the dark web, particularly some of the smaller platforms. How are you going to address the fact that if I am abroad and I cannot access my Netflix account because I am abroad, I can just switch on my VPN? How are you going to deal with the VPN, and particularly the dark web, as some of the smaller, more harmful platforms move into that realm?



HOUSE OF COMMONS

Dame Melanie Dawes: There are good uses of VPNs, as you have just described.

Chair: I do not think that is actually a good use—

Kit Malthouse: I am not sure that is a good use. Are you condoning criminality?

Chair: It is not a crime, but it is evading certain conditions.

Dame Melanie Dawes: Let me be slightly clearer. There are good uses of VPNs, such as university students who are abroad being able to access their university's portals when they are away. The Act does not ban them or give any levers on that, or age-gate them, or anything like that. Let us take the case of pornography and children. We know that most kids stumble across porn at a young age. The average age is 13 and one in 10 nine-year-olds finds porn online, which is horrific, but most of them—the younger children in particular—stumble across it, are absolutely baffled and do not know what to do and are incredibly ashamed. Having proper age verification at the age of 18 will do a huge amount to prevent those children from accessing porn.

Q52 **Kit Malthouse:** Having fought with Matt Hancock to make sure it was in the Bill I absolutely agree with you, but I am asking about avoidance. Am I able to use a VPN to get completely around the Online Safety Act?

Dame Melanie Dawes: A very concerted 17-year-old who really wants to use a VPN to access a site they shouldn't may well be able to, but a company that advertises—

Q53 **Kit Malthouse:** So that is a yes. I can use a VPN to get round the whole Act.

Dame Melanie Dawes: There isn't a technology. Individual users can use VPNs. Nothing in the Act blocks it. But—remember, we regulate companies—we have taken enforcement action against one company that said on its front page that it had geoblocked the UK, but that you can get round it with a VPN. That is not consistent with the Online Safety Act. We take a very dim view of it.

Q54 **Kit Malthouse:** So if I am offering my service via a VPN from a third-party territory, but nevertheless that contravenes the Act, you are able to enforce against me.

Dame Melanie Dawes: That is a contravention of the Act, yes.

Q55 **Kit Malthouse:** And if they are in a third-party territory and say, "Get stuffed," what can you do?

Dame Melanie Dawes: We can take enforcement action against them.

Q56 **Kit Malthouse:** But they are based overseas.



Dame Melanie Dawes: We should be clear that some of this enforcement action is going to be very difficult indeed, but already a couple of companies have geoblocked in the UK, without advertising VPNs. They are highly risky companies and decided that rather than comply they will no longer offer their service to UK users. It would be a great shame if that happened to services that we all enjoy every day in our lives, but for small but risky platforms it may well be an entirely appropriate response. There will be some that continue to take the mickey with the Online Safety Act. We should be honest that enforcing against small overseas companies intent on ignoring the law will be difficult, and at some point Ofcom will need to decide whether we pursue them through a foreign court or turn our attention to something where the risk is greater and we can achieve more impact.

Q57 **Kit Malthouse:** We could just switch them off.

Dame Melanie Dawes: We can certainly seek a court order.

Q58 **Kit Malthouse:** You can get BT, which controls the lines, to turn it off.

Dame Melanie Dawes: We are looking actively into exactly how that process needs to run so that we are ready to use it.

Q59 **Chair:** Are you transparent about that? Do you report on the challenges and issues with prosecutions? Are we aware of that?

Dame Melanie Dawes: It is only just starting.

Q60 **Chair:** But in future? You talked about reflecting new technologies, and new threats and risks, so in future can we expect to hear the challenges that you are facing, where you may need legislative or enforcement support?

Dame Melanie Dawes: We absolutely want to be clear about the realities of implementing the Act. To be honest, if there is one area where we get concerned, and where my board gets quite concerned, it is managing expectations—a sense that the Act is there, and therefore suddenly it is very straightforward and everything will be fine overnight. I do not think anyone in this room believes that. Sometimes we are concerned that the realities are perhaps not as well understood as they could be. We are very happy to talk about that, but it is very early days to be talking about the realities of prosecution. We are getting ready on all of this. We will be pushing quite hard where risks are high.

Chair: We have spent a lot of time talking about the Online Safety Act. Emily is going to move us along.

Q61 **Emily Darlington:** I have a fantastic segue. We have been talking about platforms based in other countries. There have been reports from US officials that they have met with you about the Online Safety Act and its impact on their definition of free speech. Obviously, we have our own definition of free speech, which is very long in law, predates the forming of the US and has served us well in those years. Is it true that US officials



came over to meet Ofcom to discuss the Online Safety Act, and what was discussed?

Dame Melanie Dawes: We have had a couple of meetings with members of the US Administration or from the US Congress. That is a very normal part of our work. They met Government Departments and various others in the UK as well. We are always very happy to explain our work, and that forms the major part of any of these discussions, in particular, to be clear, as I was at the beginning of this hearing, that the Online Safety Act is targeted against illegal harms for everyone, and then further protections of children, but that it does not seek to control legal free speech for adults in the way that some fear, and it does not stop anyone in the US saying anything online, provided that that is not available for British users, even if it is illegal in the UK but perhaps legal in the US, which is sometimes the case for some forms of speech. We are glad to have an opportunity to explain all of that.

We go to Washington fairly regularly. I have not done that recently, but I do it usually once a year. We talk to lawmakers from all sides of the debate. There is a lot of interest in what Ofcom is doing. Sometimes we have quite detailed technical discussions, about how you can do age verification without compromising privacy, for example. It is an important part of our job to engage in those discussions.

Q62 **Emily Darlington:** In the discussions that you have had recently and over the years, what do you think is the main difference between the approach of the UK Government and regulators to online safety and that of the US?

Dame Melanie Dawes: Freedom of speech reads differently in different countries. One of the things that we constantly try to convey is that this Parliament is pretty concerned about freedom of speech as well. It is built into everything Ofcom has to consider as a public body and it is built into the Online Safety Act. We may not have a first amendment, but we have laws in our country as well, and it is a very important part of what we do.

The other debate is the one I was just hinting at, which is privacy. There has been a lot of scepticism, including from regulators as well as people in Congress, about whether age verification can be done in a way that secures privacy. We believe it can. We have put in place rules that assume that, and we are now demonstrating it and the conversation is beginning to change. Some of the reason that there has been reluctance is a lot of lobbying by some of the companies saying that age verification can only be done at the device level. But we have the evidence. We go out and do the engagement, including with the porn industry. When things start to change in reality, you begin to win the argument.

Q63 **Emily Darlington:** Do you feel pressured in these conversations to take a more US-based approach to some of these issues than a UK-based one? Is that the purpose of these meetings, from their perspective?



Dame Melanie Dawes: No, we do not feel any pressure. It is not the purpose of the meeting from our perspective. The purpose of the meeting, from our perspective, is to explain what we are doing, because often there are misapprehensions and misunderstandings that we can try to put right.

Q64 **Emily Darlington:** Do you think there is any appetite from the US to adopt some of the UK approach on this?

Dame Melanie Dawes: The Kids Online Safety Act is live again in Congress. It is not quite the same as the Online Safety Act. It tries to do some of the same things. There is action in individual states as well. To be honest, we find that those who care about this in the US are quite pleased that the United Kingdom has acted in Parliament and that the regulator is taking it forward, because they see the UK model as one of the best ways of changing global practice. The fact that we have the English language and we are important to these companies, that Ofcom is seen as independent and objective, and that we have the right skills, experience, technology, staff and so on, is very persuasive in the industry and with other jurisdictions. People want the UK version to work because they are not entirely sure that there will be another that has the same impact.

Q65 **Emily Darlington:** Can you understand that there is some scepticism about the interactions that Ofcom is having, particularly given some of the messages coming out of the Administration about Europe and free speech and links to potential trade deals? Obviously, the Government have set this out as a red line, and we have seen that there was no softening of it in the trade deal that was negotiated with the US. Coming back to the meetings and transparency point, can you understand why that might help dispel some of the view that you are being put under pressure by another country to soften the Online Safety Act?

Dame Melanie Dawes: I would turn it around the other way. If we were allowing concerns about the view of the US Administration to stop us seeing the people whom we think we need to see to do our jobs, that would be the concern I had. When people want to come and talk to us about our work, and when we know that they may have a different perspective, we have an evidence-based, factual conversation with them about what our Parliament has asked us to do and how we are discharging that. It is important that those meetings go ahead. I understand the perceptions, but if we do not do that engagement, that is when we are kowtowing to pressure.

Q66 **Emily Darlington:** Are you being transparent about that engagement?

Dame Melanie Dawes: Yes, but at some point it starts to have a chilling effect if we explain every meeting that we are having. We have 450 people working on online safety, and it is a really big part of their job to engage with companies, with experts, with technology firms and with civil society. I honestly think that it could be quite a serious chilling effect on



us as well if we were to be asked to reveal details of every person we meet. We reveal conflicts, we reveal hospitality and things like that, but not every single meeting.

Q67 Chair: We have discussed that. You are going to come back to us with ways of addressing it.

Dame Melanie Dawes: We will come back with what we can on that.

Chair: We really need to move on. We have spent a large part of this session on the Online Safety Act. Ofcom has a wide range of powers in other sectors, particularly telecommunications, broadband and cyber-security. Now we are going to move on to artificial intelligence with Lauren.

Q68 Dr Sullivan: What is your regulatory approach to AI?

Natalie Black: First, I am glad that you have asked this question, because, of course, it is very pertinent at the moment and affects not only what we are doing in online safety but, as the Chair says, our broad remit. We have always taken a technology-neutral approach to AI, as you will be well aware. AI has been around for a long time, but the rapid deployment means that there are some important questions being asked at pace. Our regulatory approach is technology-neutral, which enables us to focus on outcomes. What are the outcomes for consumers? What are the outcomes for the market?

Specifically in the context of AI, we have tried to provide advice and guidance as early as possible to companies that we regulate and to consumers to make sure that there is transparency. You might have seen the open letter that was issued on gen AI at the end of last year. I am more than happy to talk about that. We are also working closely with academics and experts to understand how AI is changing the sectors that we regulate, particularly telecoms and the work that we do on spectrum. I am happy to take questions on any of those areas.

Q69 Dr Sullivan: Will you be using AI to help monitor AI?

Natalie Black: It is a great question, and a question that pretty much every organisation in the country is asking itself. Ofcom takes pride in being at the forefront of technology both in its serious implications for society and for the opportunities that it gives all of us. Within Ofcom, we are looking at ways that we can use AI to improve our efficiency and our effectiveness—for example, in how we give out spectrum and plan for spectrum management as well as on how we do consultations. I should emphasise that we do that very much with guardrails in place. We see the opportunities as well as the concerns. Again, like every organisation, it is about getting a balance. It is about making the most of the opportunity and making sure that there are guardrails in place, and, ultimately, that there is always a human at the end of the process.

Q70 Chair: Dame Melanie, you told our predecessor Committee that you had



the resources to cover the existing remit on AI but would face problems if asked to do more. I am unclear as to whether you feel that you are being asked to do more in terms of regulating AI.

Dame Melanie Dawes: We are not being asked to do more on regulating AI specifically at the moment; we are just being asked to implement the Online Safety Act, which, of course, requires huge regard to be had to, particularly, generative AI in that it is currently transforming services in ways that add risk and add opportunity. When it comes to the Government's AI strategy, as Natalie just said, if you try to regulate a technology, you can quite quickly end up with something that is a bit out of date. It is a bit like regulating electricity 100 or 150 years ago; it is just too broad and too whole-economy. I do not think that is something that Ofcom would be well placed to do even if it were decided that you were going to have a framework like that.

What we do as the communications regulator across all our sectors—we have to do this—is think about how AI is, as I said, transforming risk and opportunity. It is very obvious in online safety with the use of large language models and chatbots, and so on. It is also very central to how telecoms, broadcasting, the creative industries and spectrum management are developing. That is not necessarily regulating the technology, but it is having regard to how the technology is increasingly changing the regulatory challenge.

Q71 **Chair:** In the context of your existing duties, as we have discussed, misinformation is not a harm that is regulated when it comes to adults, and that applies when it is generated by ChatGPT or by AI.

Dame Melanie Dawes: Yes.

Q72 **Dr Sullivan:** In Gravesham 80% of the land mass is rural. They have a terrible time getting broadband and mobile phone signal. It really is off the grid. Gravesend has some broadband. Is it acceptable that about 50% of the premises in rural areas have access, whereas in the urban areas it is about 87%? Looking forward at the charging of BT Openreach, which costs about 20 times more for rural installation, are you looking at this as a way to help improve rural connectivity?

Natalie Black: We probably all have personal experiences of challenges in connectivity. The reality is that, if we want a successful economy and one that is focused on economic growth, we need to make sure that we have the digital infrastructure in place to support that. There is a British success story that sometimes gets forgotten. Some of you will be familiar with these stats. In 2018, only 6% of the country had access to full fibre. Today, that is 74%. The challenge, though, as you say, is often the split between rural and urban. We are seeing faster take-up of full fibre in rural areas, so, of course, that demonstrates the demand. Our role in Ofcom is to help stimulate competition to drive the build of full fibre. In the UK, we now have the fastest build of anywhere in Europe. That is something to be proud of.



HOUSE OF COMMONS

Q73 **Chair:** Fastest roll-out.

Natalie Black: Fastest build, yes, in Europe.

Q74 **Chair:** Fastest build. But coming from being behind.

Natalie Black: Hence my 2018 stat. But it is a success story. Ofcom's role focuses on those areas where it is competitive to build, where the numbers stack up. The challenge often in rural areas is that it is incredibly expensive. We work hand in glove with BDUK, which is responsible for that build-out. As a consequence, it has used some of the measures that we developed with industry—for example, using the ducts and poles required to build out broadband. Today, BDUK has provided 1 million gigabit connections, but there is still a lot of work to do. Ultimately, we need a fully connected country. We are certainly playing our part, but it has to be a partnership with others as well.

Q75 **Kit Malthouse:** In my large rural constituency, the voices have gone quiet because of Starlink. That solved the problem for lots of people. On mobile phone coverage, my memory is that it was to be revolutionised by the replacement for Airwave for the emergency services and that they were building a comprehensive 5G network, effectively, across the whole UK.

Chair: Don't take us back to Airwave!

Kit Malthouse: I do not know what the interplay is. Originally, all the masts were to be given to EE initially, and then everybody else was going to be on them. Will that not cover all those rural areas?

Natalie Black: I will not go over the history of Airwave, but the focus is on the delivery of the shared rural network. I have just been talking about broadband. You rightly raised mobile. The programme there to address the really challenging areas and notspots is the shared rural network. That was set up in 2020 when there was an agreement with the four mobile operators that, as part of their licensing requirements, they needed to build out rural coverage. That has been successful, going from about 80% to 88% across the country now. We recognise at Ofcom that the way you use your mobile has fundamentally changed, particularly over the last five years. One of the things that we are doing, actually at the end of next month, is publishing new data that consumers can use to better identify providers that are going to service them well, particularly in harder-to-reach areas. In due course, we will want to write to the Committee to explain some of that.

Q76 **Chair:** Perhaps we could have an update on Airwave. The reason I am reluctant to go there—as you are, Natalie Black—is that it was a long and tortuous experience, which I experienced both in Ofcom and as a Member of Parliament. Perhaps, to satisfy our curiosity and learn some lessons, we could have an update on that.

Natalie Black: Of course.



HOUSE OF COMMONS

Q77 **Dr Sullivan:** Can I follow up on a question that was not answered, about the cost of installation? Are you looking to review that or keep it as is?

Natalie Black: Installation in rural areas?

Dr Sullivan: Yes.

Natalie Black: Currently, that is a Government-led programme in terms of the BDUK Project Gigabit.

Q78 **Chair:** I think Lauren is talking about the regulation of Openreach in what it charges for duct and other access. That is your responsibility.

Natalie Black: Right, okay. Apologies. We are currently conducting the telecoms access review, which is a review of the market that we do every five years. As part of that, we are looking at the remedies that we have in place to make the market as competitive as possible, and that includes what Openreach charges to altnets, which are the challenger companies, to build out. Overall, it is worth reflecting that broadband in the UK is now, along with Italy, the cheapest in Europe. We have overall seen a good outcome for consumers. In terms of ensuring that the market is competitive to encourage the build that we want to see across the country, we absolutely are looking at wholesale prices.

Dame Melanie Dawes: I wonder whether when you were talking about 20 times the price you were talking about requests for people to have connections under the universal service obligation.

Q79 **Chair:** No, I think we are talking about per home. It is understandable that if the distances are larger—

Dame Melanie Dawes: Yes, it is.

Chair: It is the cost to drive it out, not the cost for—

Dame Melanie Dawes: To be clear, Openreach is not allowed to have different pricing by different area for any reason: the price is the price. Clearly, for it to pass particular homes is more expensive in some areas. It has actually done quite well, in doing more rural build than it expected. It was a condition of our review four years ago that it pass a certain number of rural homes, and it did that quite quickly. There is no question but that in some areas it is very expensive and will need the Government to step forward with funding. Those prices should not be passed on to the consumer in any event.

Q80 **Chair:** Thank you for that. For most people living in rural areas, the fact that we have some of the lowest prices for broadband is not going to be helpful. I recognise that it is a good outcome overall, but for the country to have the ubiquity of access that will drive economic growth and skills, we also need to take very seriously the challenge of rural broadband. I think what you are saying is that you are doing so, but not through the regulation of Openreach pricing.



HOUSE OF COMMONS

Natalie Black: If I may add, Chair, one of the things that we are doing at Ofcom is helping to stimulate innovation in this area—for example, direct-to-device communication, which will help rural areas. Some of you might have seen recently the example of the satellite video call that was done by Vodafone. That was enabled by an innovation licence granted by Ofcom. We have granted over 760 innovation licences. It is the combination of things that we can do. It is the regulatory levers that we have and making the most of those. It is also about playing our part in the innovation economy and giving, particularly, companies in the UK the opportunity to come forward and try different things.

Chair: That is very interesting. I knew that we would be spending a lot of time on the Online Safety Act, and then we would have less time to consider all the other important and interesting things that you do, such as innovation in rural broadband. Do we have a hard stop at 11.30? The session is planned to go on until midday.

Dame Melanie Dawes: We are in your hands.

Q81 **Chair:** Excellent. We may take a bit more time, then. You have talked about stimulating competition, which is part of your remit. You have also said that by 2031, which is only six years away, “if effective competition has developed, there will be no need” to regulate Openreach. Can you tell us what you mean by effective competition and how likely it is?

Natalie Black: What we are looking at through the telecoms access review, which I mentioned previously, is how we see sustainable competition developing in the market. The outcome that we are trying to achieve is full fibre roll-out across the UK, and to do that we have stimulated competition. Openreach is building, as are challenger companies, of which there are now many in the UK. We look across the UK to see where there are more than one or two challengers appearing. Previously when we looked at this, nearly five years ago, 70% of the country had potential sustainable competition. Now it looks like 90%. We have set out in the telecoms access review a signpost that when it comes to 2031—

Q82 **Chair:** Let us just clarify this. You are saying that in 90% of the country it is possible that you would have two to three fibre networks to your home.

Natalie Black: At least one alternative to Openreach.

Q83 **Chair:** Two fibre networks to your home.

Natalie Black: At least one alternative to Openreach, and in some cases—

Q84 **Chair:** Does one plus one not equal two?

Natalie Black: Apologies if I am not clear. When we look at the roll-out from companies in terms of their plans for the UK, as an alternative to Openreach we see that now in 90% of the country there is the potential



HOUSE OF COMMONS

to have one alternative, and, actually, in many other parts of the country, it could even be two.

Q85 **Chair:** To clarify, this is with Openreach having already rolled out or already having a connection. It is two physical connections to the home.

Natalie Black: Yes, exactly.

Q86 **Chair:** So it is not using the same pipe.

Natalie Black: In many cases, it is using the same pipe, yes, because that is part of our—

Q87 **Kit Malthouse:** I find that unbelievable. The whole of north London only has one.

Dame Melanie Dawes: When we say that fibre is available, it would usually be passing the home in the ducts or poles down the street or overhead—

Chair: Oh, okay. Within 20 yards.

Dame Melanie Dawes: And then the customer might decide to switch network. That is something we have put in much stronger requirements around: switching networks, so not just retail provider.

Chair: The ability to switch network.

Dame Melanie Dawes: But that is when you get it hooked up to your wall and—

Q88 **Chair:** There is a little bit of scepticism that 80% to 90% of the country can have two connections.

Dame Melanie Dawes: It is already 70%.

Q89 **Chair:** This is by households, not by geographic area.

Dame Melanie Dawes: Yes.

Dr Sullivan: Many do not have a connection.

Natalie Black: Please can I emphasise that it is potential? What we are doing in the telecoms access review at the moment is trying to anticipate what the market will look like by 2031. To do that, we have talked to all the companies that are operating at the moment and reviewed their plans, but it is potential.

Q90 **Kit Malthouse:** Is that FTTP or FTTC?

Natalie Black: FTTP, fibre to the premises.

Kit Malthouse: Two possible connections. I find that unbelievable.

Q91 **Chair:** By 2031. And only if that happened would you then consider not regulating Openreach.



HOUSE OF COMMONS

Natalie Black: The test for us is sustainable competition, and there is a whole range of factors that we would need to look at. This is looking some time ahead—to 2031.

Dame Melanie Dawes: It is not about no regulation either. We will have to judge where there might still be significant market power for Openreach and where there is not. We are increasingly confident that in large parts of the country there will be at least some competition on a long-term basis.

Chair: That is very interesting.

Q92 **Martin Wrigley:** The numbers that you just talked about have given us some perplexion. Could you possibly back that up with something in writing to us, please?

Dame Melanie Dawes: Of course. I am very happy to.

Q93 **Chair:** That is a good point, Martin. To come on to another aspect of Ofcom's regulation of Openreach, you said that Openreach should not incur unnecessary costs for running two networks at the same time. You are basically talking about the PSTN switch-off, aren't you, which has caused a lot of concern? There have been tragic cases of the elderly and vulnerable who have been left without access to emergency services. How much is Openreach going to save from turning off the PSTN? How are you ensuring that it is done safely and with consideration for wellbeing, particularly, of the vulnerable? There has not really been very much information about it, has there?

Natalie Black: First, I am glad that you have raised this, because it is a very difficult and complex problem, and, as you say, Chair, there have been some very sad cases associated with it. There are about 5 million people still on the PSTN, so there is quite a sustained programme of work. We have been working very closely with Government to make sure that it is done carefully. You will be aware that the programme was paused last year and the Minister, Chris Bryant, developed a checklist for non-voluntary transfers to make sure that the right measures were in place.

Q94 **Chair:** Would you agree that before that pause, it was not being done carefully and there was not sufficient requirement to work with Government or to inform consumers?

Dame Melanie Dawes: The history, which I recall certainly from 2020, is that Ofcom put in place guidance to the industry as early as 2018, I believe, that said that you must take care to protect vulnerable customers.

Q95 **Chair:** Either that did not happen or—

Dame Melanie Dawes: What did not happen was that there was not very much switch-off of the PSTN in the early years. In 2022, we began to get very concerned that BT's transition was not going well and that



HOUSE OF COMMONS

they were not sufficiently aware of what it was like for customers who had signed up to fibre and did not realise that their PSTN phone line was going to be switched off at the same time. We had some quite serious conversations. I had some of those with the senior management at BT, and they paused their migration at that point and reset it.

Q96 **Chair:** It was not working and then it was paused.

Dame Melanie Dawes: No, it needed a lot more attention than it was getting. What the Government have done more recently has had another impact. It is 5 million consumers, but a lot of those for whom it is easy to switch have now already done it. You are increasingly getting into a more vulnerable group.

Q97 **Chair:** More difficult. How much—

Natalie Black: I want to come back to your question. I am afraid I do not have that number to hand, but I am very happy to follow up for you.

Q98 **Chair:** Okay, that is great. There are obviously ongoing concerns about the impact of switching off the PSTN. I would be very interested to hear how you see that evolving.

We are going to move to another area where Ofcom has a huge responsibility, which is the risks in relation to cyber-security and resilience. I am particularly interested to hear that Ofcom received only one reported incident in 2022, and none in 2021 and 2023, with regard to cyber-security and resilience. As you mentioned, we have seen attacks on the retail sector. Is it that they are not attacking our telecoms networks, or is it that they are not being reported?

Natalie Black: I might clarify that, if that is all right, Chair. If I have understood correctly, that one notification will be under NIS, the Network and Information Systems—

Chair: Yes.

Natalie Black: But we are also responsible for implementing the Telecommunications (Security) Act, and we have had a lot more notifications in that space. The NIS is relatively narrow in its definition; it focuses on digital infrastructure. We regulate a small group of companies under that legislation. The Telecommunications (Security) Act is where our real cyber powers sit. We regulate 40 companies there, and we have had 15 notifications that relate to denial of service and ransomware, the typical things that, unfortunately, you see in cyber-security attacks.

Q99 **Chair:** We will come on to network security in the telecoms sector specifically. When it comes to the NIS notifications, do you feel that one in three years is a true reflection of the resilience and security of the networks you regulate?

Natalie Black: I will be honest, I am quite new in this job—I have been in place for six months—and I certainly found that interesting, but you



will be aware that the cyber security and resilience Bill coming forward will change the definition and scope of some of the NIS requirements. We welcome that. The challenge is that this space is moving quickly, so trying to stay ahead of the threats is quite difficult. One of the opportunities that is coming up in the cyber security and resilience Bill is that scope will not have to be amended through legislation, which will give us more flexibility.

Q100 **Chair:** You have seen that in the cyber security and resilience Bill.

Natalie Black: I understand that is being required.

Chair: I do not think we have seen that.

Q101 **Martin Wrigley:** I am struggling to keep up. It has been quite a while since I was building telecoms networks, having started in the early '90s with Orange UK. You spoke earlier about reports of breaches. Do you think the network is taking it seriously?

Natalie Black: In terms of how we engage with the companies and what we have seen, yes. As part of the requirements under the telecoms security Act, we wrote to the Secretary of State at DSIT earlier this year. Our view was that we are making progress. They are taking the requirements seriously, but there is a lot more to do. The nature of the threat is changing; the way technology is being used in telecoms is changing, going back to our point about AI. There are very real-world implications, as we all see only too well at the moment. In summary, I think they are taking it seriously, but there is more to do.

Q102 **Martin Wrigley:** How do you get a picture of what is going on, and what sort of steps are you taking to make sure it is moving fast enough to keep pace?

Natalie Black: First, I should emphasise that this is a partnership approach. We work very closely with Government, but we work particularly closely with the National Cyber Security Centre. They drafted the codes of practice that we are responsible for monitoring. They share information with us about how the threat environment is changing. We have ongoing dialogue with all the relevant companies—as I mentioned, there are 40—under the telecoms security Act to understand how their networks are developing and the kind of threats they are seeing, and we encourage sharing across the sector. Again, the NCSC plays an important part in that.

Q103 **Martin Wrigley:** Would the development of shared networks and network infrastructure, which is what I imagine is going on there, complicate it, or are the responsibilities clear in that for cyber-security?

Natalie Black: The responsibilities are very clear. The NCSC plays an excellent role in convening all the different interested parties. Undoubtedly, the nature of digital infrastructure is becoming more complicated, as we have just seen in Spain and Portugal in some of the



resilience issues taking place there. We are not at all complacent about how challenging this is.

Q104 **Emily Darlington:** I want to come back to the cyber security and resilience Bill. You are obviously looking to future technology development. I want to understand your assessment of the current risk level on cyber-security, in particular in relation to foreign actors.

Natalie Black: The Government obviously set the threshold and GCHQ is the lead. Through the NCSC, it then communicates that to all interested stakeholders, but, at least from what we see at Ofcom, there is a lot of activity by nefarious actors. That can be quite wide-ranging both in impact and where it affects digital infrastructure.

Q105 **Emily Darlington:** Where do you see the greatest weaknesses in the areas that you look at?

Natalie Black: First, through the code of practice we work hand in glove with the National Cyber Security Centre and recognise, as is quite familiar across infrastructure, whether that is in telecoms or other parts of the economy, that, as ever, it is your own employees, so it is making sure they have the necessary training and, for example, are using two factor authentication. Secondly, it is the design of the infrastructure, designing security from the beginning so that it is not an add-on. Thirdly, I would probably highlight the use of third-party suppliers, which is always challenging. That is one of the areas that we look at through the telecoms security Act.

Q106 **Emily Darlington:** In your conversations with DSIT on the cyber security and resilience Bill, do you think those three areas of potential weakness are being properly addressed?

Natalie Black: To be clear, when we say weakness, those are threats we see across the economy that are evolving all the time.

Emily Darlington: They are the soft points.

Natalie Black: Exactly. There are measures in place already through NIS and the telecoms security Act, but the cyber security and resilience Bill is an opportunity to make sure that we do not rest on our laurels and that we evolve both how we look at these threats and the powers we have to deal with them. That is a long way of saying we can always be better in this space. That is the challenge of cyber-security.

Q107 **Emily Darlington:** This is your opportunity to lobby lawmakers. We will have to vote on the Bill. From your perspective, what do we need to be looking at to give us hardening of those soft zones, in the cyber security and resilience Bill?

Natalie Black: Melanie might want to come in here, but I would start by saying that it is a team sport and the fact is that we all have to work together in partnership. The Bill is an opportunity to make sure that



everyone involved has the powers they need. That would be one thing to look at.

Dame Melanie Dawes: Our expectation is that the Bill will look at new sectors, such as data centres, that need to be covered, as well as at how the existing rules are working. We have said to Government that we are happy at Ofcom; we can do more in some of these spaces to build on the capability that Natalie and her team already have on telecoms security. We can do a bigger role on NIS. I think that this morning Chris Bryant will be confirming that they are going to ask Ofcom to take on the data centre role. Other regulators will take on other parts of the expanded NIS regime. It is very much a multi-agency approach. The GCHQ and NCSC role is so important. To bring home what Natalie has already said, the Government write the codes of practice for the telecoms security regime, not Ofcom as regulator. Our role is to implement, because they are the ones who have the understanding of the threat. I think that will thread its way through the new rules, and it is the right approach. Clarity about roles and responsibilities is always important as we are getting legislation right.

Q108 **Emily Darlington:** We are the Science, Innovation and Technology Committee, so we love to talk about new and exciting emerging technologies: quantum technology, 6G and the increasing importance of satellite technology when it comes to telecoms. Do you think that the cyber security and resilience Bill has a proper understanding of and is future-proofing for these emerging technologies, which have fantastic potential?

Natalie Black: As a personal view, I do not think there is any such thing as future-proofing; it is the environment we live in. Instead, it is about making sure the UK is at the forefront of innovation. You mentioned 6G, for example. Ofcom is looking at how we will deploy the upper 6 GHz band to make the most of the potential opportunity for 6G going forward. You mentioned quantum. We work hand in glove with the National Quantum Computing Centre, which you will know well. That is how we operate at Ofcom; we look both at the opportunities and at making sure we are addressing the challenges side by side. That is how we look at them in my team—across the full waterfront.

Q109 **Emily Darlington:** The point about satellites is really important, given that it can be a national security issue and a cyber-security issue with the connection to telecoms. Do you want to say anything about the nature of some of the behaviours of satellite firms that present particular challenges in those areas?

Natalie Black: Through our spectrum team we work with the satellite companies. There are currently eight lower-orbit satellite companies licensed through Ofcom in the UK. There is only one operating that provides broadband, which has already been mentioned. When you think about the telecom strategy for the UK, inevitably satellite has to play a big part in that, for all the reasons we have mentioned about rural



HOUSE OF COMMONS

communities. We are thinking about what needs to be the long-term strategy to ensure we get the best for British consumers. As you say, there are some behaviours there, but we are used to dealing with those in other elements of our remit. One of the great strengths of Ofcom is that these companies now operate in many different parts of the UK economy and we get to see them, understand their behaviours and have the expertise to deal with them because we now have so much experience in that space.

Dame Melanie Dawes: Lower-orbit satellites are a scale business. There are serious competition issues, but they are global ones. Ofcom represents the UK in close collaboration with the Government in the ITU and in world radio congresses, as you know. We are strong in those fora; we are recognised for our technical expertise and we have a good team there, but fundamentally there are some big debates to play out between the traditional satellite operators and the new players, and some big questions of competition. What we are doing in the UK is making sure that when we license operators in the UK we put in conditions that mean that at local level competition is provided; for example, if you have a satellite in one home it is not configured in a way that prevents another operator from selling one to the neighbour. We are doing what we can at local level. In the end, competition does not always work, but it is a good cleaning and transparency mechanism that can help. I am not saying it cures everything.

Emily Darlington: I completely agree. We need a high seas of the high space, or whatever we want to call it.

Chair: It may be an issue for science diplomacy as well.

Emily Darlington: Exactly. I agree.

Q110 **Chair:** I want to follow up with two specific questions in this area. It is not really a new technology, but the internet of things is obviously a telecommunications system and covers everything from toothbrushes to smart meters and, increasingly, autonomous vehicles. Does Ofcom regulate the internet of things?

Natalie Black: No, we do not, but there will be touchpoints that affect some of our frameworks. You mentioned smart meters. For example, smart meters predominantly connect through elements of 2G and 3G at the moment. As part of the 2G/3G switch-off, we are working with Government to understand the impact. We do not have broad-ranging commitments, but it certainly interacts with our work.

Q111 **Chair:** So you do not regulate the internet of things in the extent to which it communicates with non-2G or 3G or Bluetooth.

Natalie Black: No. It would be the interaction with the telecoms system.

Q112 **Chair:** That is interesting. One of the requirements under the telecoms security Act is to reduce supply chain risks. Does Ofcom take a role in



looking at supply chain risks?

Natalie Black: Yes, we do. It is one of the measures under the code of practice.

Q113 **Chair:** How are we doing in reducing supply chain risks? We have the example of Huawei being torn out of our systems, which is extremely painful and costly. Are we heading for another such problem?

Natalie Black: You will be aware that the Government set out that Huawei needs to be removed from 5G kit in the UK by 2027. The role of Ofcom there is to support and monitor. A number of companies identified by the Government have to report on how that is progressing. The Government take a whole view; we provide the monitoring support there. You are right to highlight that supply chain risk is an ongoing issue. That is the case that gets a lot of attention, but there is a whole range of supply chain threats that also need to be considered.

Q114 **Chair:** Are you monitoring them?

Natalie Black: We are doing that through the telecoms security Act as far as we can, but my understanding is that with the new cyber security and resilience Bill there will be additional measures for supply chains.

Q115 **Chair:** What do you see now as the biggest supply chain risk?

Natalie Black: Probably third-party vendors. Again, with the very live cyber-security incidents, that is something that a lot of experts are talking about. Whenever you are building infrastructure it is always difficult because you cannot control everything, and it is your interactions with third parties that are challenging.

Q116 **Chair:** We have two or three further questions looking generally at Ofcom and its funding. Dame Melanie Dawes, you have marked five years in your role as chief executive of Ofcom. Congratulations. How would you rate your performance, and how long do you expect to remain?

Dame Melanie Dawes: I think it is for my board and others to judge my performance.

Chair: A very diplomatic answer.

Dame Melanie Dawes: I love this job. It is incredibly interesting, and what we do is really important, definitely over the next few years on online safety and in other areas such as the telecoms access review, satellite and our work on public service broadcasting. For me, there is a lot that I still want to be part of. I work with brilliant colleagues. My board supports me in that.

Q117 **Adam Thompson:** Let me move on to the upcoming spending review. At the moment, in your view, are you under pressure from the Government to cut costs as part of that review?



HOUSE OF COMMONS

Dame Melanie Dawes: Because Ofcom is funded by fees, either from our industries or through spectrum licences, we are not part of the public expenditure framework, so we are not part of the spending review process at the moment. We have had discussions with the Government about our budget for the next few years. We have concluded what we believe to be a satisfactory outcome to that, which allows us to get on with the job.

The context is that since 2009 we have had a flat cash budget in all but one year, up until the year just finished, on our traditional core Ofcom work. Where we have had new duties we have had extra funding, but the core has been flat. When you bring in new duties it enables you to be more efficient because the overheads can be shared more widely, so that is always useful for us. We have had to make significant efficiencies; it is a 40% overall cut over that period. We have done that by consolidating our estate, with significantly fewer floors in Riverside House, which the Chair may remember from her time at Ofcom in the early 2000s, and all the things you would expect around contracts, expenses and other parts of corporate costs.

Q118 **Chair:** Just to clarify, you have agreed your spending cap with the spending review. While you raise money through fees, there is an overall spending cap that covers everything.

Dame Melanie Dawes: There is an overall number and within that the online safety budget is separately identified, because the fee regime has not come in yet.

Q119 **Adam Thompson:** On the online safety regime, I understand that the Government are funding it until it is up and running in 2026-27. Do you have any ideas about whether that will be impacted in the spending review?

Dame Melanie Dawes: We are not expecting it to be impacted in the spending review. Obviously, what we have to do is get the fee regime in place. This is about asking some big tech companies to pay our costs. We have not done that before.

Q120 **Chair:** I think Facebook's revenues are 1.3 trillion. How much do you think you will be asking them to pay you?

Dame Melanie Dawes: Overall, our online safety budget for next year is £72.5 million. In subsequent years it will be broadly flat from here on in, with a small inflation adjustment. We are reasonably stable, at least for now, in our funding. That will be paid for by the companies we regulate, particularly the larger ones. To finalise that, we have to do the statutory instrument on the thresholds above which you should come into scope—we do not want lots of very small companies paying small amounts; it will be a small number paying large amounts—and the statements of charging principles and so on that go alongside that. We are expecting to finalise that in the next few weeks, probably after the parliamentary recess.



Q121 **Adam Thompson:** Do you have an idea of approximately where those thresholds are likely to be? How big are the companies we are looking at?

Dame Melanie Dawes: We have set out proposals for consultation, and I am happy to confirm that. It may be best if we just send you what we are going to do and when in the next few weeks, and we are happy to explain it, if that is helpful.

Adam Thompson: We would appreciate that.

Q122 **Chair:** I have a couple of questions about growth. There is a requirement placed on Ofcom to support the Government's focus on growth. In the response to the Government's request for ideas to boost economic growth you mentioned the need for regulators to innovate. What innovations is Ofcom currently undertaking to boost growth?

Dame Melanie Dawes: It is in two parts. The first is how we innovate in our regulation. The best example is the work we have done on spectrum licensing over the last few years. For example, to license the direct-to-device pilots that Natalie talked about earlier has required a lot of innovation from our teams, thinking how to do that. Normally, when you license spectrum you are licensing a fixed UK-based on-the-ground installation, so we have had to find creative ways to go round that. As Natalie said earlier, we are supporting through sandboxes and so on new ways of using spectrum so that we can stay ahead of the curve. Innovation is absolutely central to that area of Ofcom's work.

More broadly on growth, what we are doing on fibre roll-out is absolutely central to the economy in so many different ways. We believe we contribute a lot to the future productive potential of the economy to serve citizens and consumers in the future, not just today. Our overall duties are cast broadly, which allows us to take a rounded view when we make decisions, going back to broadband, and prioritise investment in this period, not just prioritise the lowest possible prices. We feel very enabled as a regulator to prioritise growth, but we welcome the challenge of whether we are doing enough. We are constantly working on it. Our board has taken it very seriously as well.

Q123 **Chair:** That is very good to hear. In your response you referenced highly valuable spectrum awards as a growth-driving measure. You just mentioned the direct-to-device spectrum. The last award raised just over £1 billion. Would you expect to raise much from any future awards that might help fill the Chancellor's spending requirements?

Dame Melanie Dawes: That was the 5G spectrum back in 2021, I think. We do not have targets for pricing. The whole point of an auction is that it is a widely internationally recognised way of allowing an industry collectively and fairly to bid and set the price for scarce assets. Maybe. I would expect that particularly where we are auctioning high-in-demand spectrum there will be revenue for the Government coffers.



HOUSE OF COMMONS

Natalie Black: We have 1.4 GHz coming up this year, as well as high capacity, but it is not just the metric you mentioned in terms of how much is raised from the spectrum auction; it is also an enabler more broadly. For example, when we look at shared use of 5G, as Melanie described, some of the innovations we have done there have enabled the growth of private networks for companies like JLR in Solihull to do advanced manufacturing in a way that was not possible before. I suggest that those are two metrics you would want to look at there.

Chair: The amounts raised and how they drive technology roll-out and specifically increased productivity. How Ofcom is driving not only fundraising for the Government's coffers but productivity is a very good note on which to end. We have talked about a wide range of subjects within Ofcom's very wide remit, and I thank you for giving your time to us today. It has been extremely interesting. You have taken us through your wide remit. Dame Melanie Dawes, you say you love your job. I hope you do too, Natalie Black. Can I add that it is great to have an all-female panel? It is not something we often get when it comes to tech panels. I am glad that you both enjoy your jobs. You have very challenging roles and we really appreciate your sharing with us the challenges and opportunities that you face. Thank you.