HOUSE OF COMMONS

Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation

Oral evidence: Online safety and online harms, HC 620

Tuesday 26 October 2021

Ordered by the House of Commons to be published on 26 October 2021.

Watch the meeting

Members present: Julian Knight (Chair); Kevin Brennan; Steve Brine; Alex Davies-Jones; Clive Efford; Julie Elliott; Damian Green; Simon Jupp; John Nicolson; Jane Stevenson; Giles Watling.

Questions 34 - 148

Witnesses

I: Andy Burrows, Head, Child Safety Online Policy, NSPCC; and Susie Hargreaves OBE, Chief Executive, Internet Watch Foundation and Director, Safer Internet Centre.

II: Seyi Akiwowo, founder and director, Glitch; Rt Hon Maria Miller MP, former Culture Secretary and Minister for Women and Equalities; Marianna Spring, specialist disinformation and social media reporter, BBC; and Cordelia Tucker O'Sullivan, Senior Policy and Public Affairs Manager, Refuge.

Examination of witnesses

Witnesses: Andy Burrows and Susie Hargreaves OBE.

Q34 **Chair:** This is the Digital, Culture, Media and Sport Select Committee and our sub-committee hearing into online harms. We are joined for our first panel by Andy Burrows, the Head of Child Safety Online Policy at the NSPCC, and Susie Hargreaves OBE, Chief Executive, Internet Watch Foundation and Director, Safer Internet Centre. Susie and Andy, thank you for joining us this morning. We are very grateful that you have been able to attend, particularly as you are attending in person. It is still always a bit of a novelty.

To Susie first and then I will ask Andy's opinion as well: do you think the draft Bill delivers on its overall promise to address content that is harmful to children and, if not, why not?

Susie Hargreaves: Thank you very much for inviting me today, Chair. I think it can deliver on making online safety better for children. At the IWF I deal with illegal content and in the organisation I work for we deal with child sexual abuse content. We have a number of key recommendations we would like to see within the Bill. I think it is important to frame that in the context of what we mean by illegal content. We are talking about child sexual abuse where there is clarity in law.

The IWF has been going for 25 years and we have a world-leading approach to dealing with child sexual abuse online. Since we started, less than 0.1% of child sexual abuse is hosted in the UK and that is down to the superb relationships we have with law enforcement, the industry and Government. To understand the scale of the issue, last year we removed 153,000 webpages of child sexual abuse; that is millions of images. One of the issues that we want to talk about is that it is not that the job is done—there is still a huge threat to children out there. The NCA's current estimate is that there are between 500,000 and 850,000 people with a sexual interest in children in the UK. We need to build on the successes of what we have been able to achieve so far and we think this Bill provides the opportunity to do that.

However, at the moment so much of it is dependent on the secondary legislation, so the detail in the Bill is going to be really important. There are three areas where we think it needs further clarification. The first is that when dealing with illegal content we need to ensure that the processes and systems that are put in place continue to be effective. I say continue to be effective because under section 9 of the Bill where companies are required to minimise the spread of illegal content and minimise the amount of time that content is available, these are all mechanisms that are currently in place. We currently have a situation where we are able to bring down content incredibly quickly and are held up as a world model to do so. We need to ensure that the Bill does not become a Christmas tree Bill, that it does not lose focus, particularly on child safety and, for us, illegal content, and that we make sure that the

processes and the expertise we already have in this country are built upon and not minimised in any way.

The second point linked to that is we need clarity around the co-designation in the Bill. We know that Ofcom will be dealing with a multitude of harms. We have clarity in law on illegal content, so we need to ensure that we work with experts—and I put the IWF forward for that—and we would like to see a lot of further thought on areas in the secondary legislation, because a lot of decisions are left to the code of practice or the Secretary of State on illegal content. The role of the co-designators is crucial.

The final big issue for us is that the legislation needs to have effective integration with law enforcement. When it comes to dealing with illegal harms—and particularly for the IWF where we have an MOU between the Crown Prosecution Service and the National Police Chiefs Council, and we provide an absolutely essential brokering relationship between the internet industry and the Government and law enforcement—we need to ensure that that is not lost within the Bill and that some focus and priority is put on dealing with illegal harms.

Andy Burrows: Good morning, everybody, and thank you for the opportunity to give evidence today. Child protection should be a key focus for this legislation. It was the impetus for the original commitment to legislate and I think it is one of the core areas on which this legislation will be judged eventually. I agree with Susie that the legislation can, and indeed must, be a game changer for child protection. It is a very complex Bill and it has a difficult task to achieve in balancing the range of fundamental rights at stake and balancing safety with other objectives. I think it also boils down to a fundamental choice about whether the legislation will do everything that is reasonable and proportionate to prevent what is inherently preventable abuse taking place and being facilitated on online platforms.

Our assessment is that the Bill is a good starting point but there are some substantial areas where we would like to see it strengthened in its ambition to ensure that it truly can protect children from inherently preventable harm. There are a few core areas that are priority concerns for us. First, we think the Bill needs to map more effectively on to the dynamics of the child abuse problem. We know that child abuse is a cross-platform issue but the Bill at present is not constructed in a way that the duties will apply in that respect. We think the measures around the child safety duty need to be bolstered, and in particular we have concerns that the thresholds there are higher than both the video-sharing platform regulation and the children's code so that the level of protection as it stands could be weaker.

It is vital that this regulation is future proof and agile, and I think there are questions about whether it will achieve that with how the drafting is currently constructed.

Q35 **Chair:** Sorry, Andy, what do you think of the fact that there is five days between the end date for the Joint Committee and the Prime Minister making a pledge that this will come before the House? You must be worried, as someone with concerns for the safety of children, about a five-day turnaround to draft important legislation.

Andy Burrows: I think the emphasis absolutely should be on making sure that this legislation is as effective and robust as it needs to be. Clearly five days is deeply challenging, to say the least, to ensure that there can be effective—

Chair: You are being very kind—"deeply challenging" means it is nonsense, doesn't it?

Andy Burrows: We would rather see the time taken to make sure that this legislation is as effective and robust as possible before it enters into—

Q36 **Chair:** Do you think a date of maybe March rather than before Christmas would be best for the protection of children, that the Government should not stampede it for five days and that by so doing there is the potential of putting children at risk?

Andy Burrows: We can certainly say that legislation is rarely strengthened by being rushed and we need to make sure that we get this right. Ultimately we need to have a piece of legislation that will act as an effective part of the child protection landscape for decades to come. If that means a couple of extra months to work on the detail—

Q37 **Chair:** Five days. I know that you have relationships with the Government, and we all have around this table, but at the same time there is a certain amount of—let's be frank about this—open-mouthed incredulity about the idea of five days between the end date for the Joint Committee and the presentation of a Bill to the House of Commons. Andy, as someone who is charged with the idea of protecting children in our country in an esteemed charity, you must be really deeply concerned about that timetable.

Andy Burrows: We certainly question whether five days is in any way feasible to be able to bolster this Bill in the way that is required. The timescale that you have suggested of moving this to the spring, if that gives the time to make this legislation right, is time well spent.

Q38 **Chair:** Susie mentioned that only 0.1% of child abuse content is hosted in the UK but yet 153,000 pages are taken down each year. Was it each year, Susie? It was, wasn't it?

Susie Hargreaves: No, year on year we have taken down more and more. When I say less than 0.1% hosted in the UK, over 70% is hosted in the Netherlands. We are great at not hosting content in the UK; we are not great at not looking at it.

Q39 **Chair:** Andy, in your view will this legislation effectively reverse that

trend of people seeing more child sexual content online?

Andy Burrows: I think the legislation needs to avoid falling into the trap—and indeed when Ofcom is taking decisions—that the upper limits of what is possible or necessary is what the largest platforms do currently. We need to ensure that this legislation is absolutely outcome focused and the outcome that we are trying to achieve here should be trying to disrupt and prevent the ways in which child abuse can be viewed but also circulated. We know that in particular social networks and gaming platforms act as the start of a conveyor belt on which new images are being produced, as well as existing images, then being shared, and broadly successfully taken down.

We need to see a robust set of responses in the legislation. When Ofcom starts to construct its regulatory scheme we need to see a very proactive approach with clear and reasonable expectations on companies that they should not be hosting child abuse but also they should be taking design choices wherever they can to ensure that their products frustrate the ease with which at present abusers are able to use services to groom children and to produce new images.

Chair: Is that a yes or a no, Andy?

Andy Burrows: As it stands, we think the legislation needs to be more ambitious if it is going to hit that objective.

Q40 **Chair:** You mentioned about cross-platforms and you intimated that the basic effect is simply that first indications of child sexual abuse sometimes come through gaming, through the potential of viewing someone playing a game online I presume, but those are not tier 1 platforms. They are not on the tier 1 system, are they? When it comes to this particular area of acute harm, which everyone must agree is something that is absolutely, along with terrorism, the most vital area to crack down on, what is your perspective on whether or not the tier 1 and tier 2 system is adequate to prevent these 153,000 pages being uploaded and viewed?

Andy Burrows: The solutions need to map on to the dynamics of the problem with the expectations on companies to try to disrupt abuse that is taking place on their sites and also with the transparency arrangements that will apply. What we are talking about here on gaming platforms and on social networks are very well established and understood grooming pathways in which abusers will exploit the design features of the services, the communications features, to look to migrate children on to other platforms. The response needs to be proactive but it needs to have that cross-platform articulation of the safety duties.

Q41 **Chair:** These individuals will simply avoid tier 1 platforms. They will go to other ones and meet children via gaming, filming them, and then they will say, "Why don't you meet me on this one, why don't you meet me on that one?", one of the obscure ones. How on earth do we catch the tail of this particular tiger?

Andy Burrows: You are absolutely right. If the outcome of this legislation is that harm is not tackled or it is misplaced, we would be missing an opportunity to protect children. We need to see a broad, overarching safety duty that places clear requirements on all platforms to consider the impact of their own design choices but also how their design choices and their services fuel this harm ecosystem. No one platform will have all of the pieces of the jigsaw about how harm perhaps starts on their site and then migrates elsewhere, or starts on another site and then migrates on to their platform.

It is important for us that we can see the safety duties being applied on this cross-platform basis. That means in practice that there are mechanisms for platforms to be sharing threat intelligence—to come together and to share an understanding of a very agile and evolving threat, and for there to be mechanisms in place for rapid response where there is substantial harm taking place. Companies who are actively trying to do this now use a very ad hoc process. It may be as simplistic as you happen to know someone who has moved to a different firm and so you can pick up the phone and speak to them to understand a very agile and changing threat. The objective here should be a systemic response and we cannot have key parts of it being ad hoc.

Q42 **Chair:** That means data sharing across not just tier 1 but everywhere?

Andy Burrows: There is a real role for data sharing and I do not underestimate the challenges in making sure that we can do that effectively. DCMS is doing some good work to explore what that could look like, but I think that has to be a key part of the regime. I doubt very much that that will happen unless we see the sector working together on harm and having clear responsibilities.

One of the important points in cross-platform risks is how we mitigate the potential negative interplay with competition law. Having a clear articulation of the safety duties applying on a cross-platform basis in primary legislation feels like the most effective way of doing that. The other routes to achieving that, for example carve-outs to section 1 of the Competition Act, tend to be much more time limited, so less suited to what will be an ongoing task.

I think it is absolutely vital that we see this built into the primary legislation. In turn, this gives Ofcom the comfort of understanding the boundaries of its remit rather than being in a situation where it is potentially subject to future challenge or being contested.

Q43 **Chair:** Susie, you have heard what Andy said about the need to have data sharing across platforms but also a need for Ofcom to have the sinews, the power to be able to stretch out beyond tier 1 to establish processes to clamp down on this appalling imagery. What are your thoughts on what you have heard from Andy? Do you think that the legislation as it stands at the moment is a way of achieving that?

Susie Hargreaves: We recognise that cross-platform is an issue, but it is important to bear in mind that all the technology companies are different, the technology is different. They do not have a magic switch that they can just apply from one company to another. I think we need to acknowledge the fact that they currently share a lot of data and I can give you an example. We are dealing with imagery, not text, and in grooming a lot of the text encouraging children happens on networks that we are not dealing with, but when it comes to imagery we have hashing technology. We put digital fingerprints on known images and these are shared by the industry and the National Center for Exploited and Missing Children in the US. We are currently assessing and hashing 2 million child sexual abuse images in the national Child Abuse Image Database. That hashing technology was created by Microsoft PhotoDNA, and companies use and share other hashing technologies.

That is not to say that companies cannot do more in sharing information and intelligence, but the companies that work with us take our services and they share a lot of this information. We need to ensure that we recognise the good stuff that does happen, because without the engineers from the technology companies we are not going to have the means and the engineering to share a lot of this data. That is one thing.

It is important to recognise that Ofcom needs to know what it is investigating. It does not necessarily have the means to understand what the problems might be on the technology, and that is why it needs to work with experts in the field and harness expertise so that it can understand that.

The final thing on this is that of course we are talking about an international problem. The issue of hosting is an interesting one because the Online Safety Bill, which is being looked at throughout the world, will not necessarily resolve the issue we have with hosting because it is all hosted in the Netherlands. What you need there is the Netherlands to step up and develop a zero tolerance approach to hosting.

Q44 **Chair:** Wouldn't it just be hosted in Ukraine?

Susie Hargreaves: The argument is that we have removed hosting in the UK and therefore we just pushed it—

Chair: Not the UK, Ukraine. Wouldn't it move somewhere else?

Susie Hargreaves: Yes, I know. We just pushed it to another country. I do not accept that because if every country stepped up and said, "We are not going to host this and we have it removed immediately" there would not be anywhere for it to hide. The reality is we play a bit of a whack-a-mole game in getting it removed. It may jump to another country but that is not a reason to leave it up there in the Netherlands because these are children who are being sexually abused. It needs international co-operation.

Q45 **Chair:** I am not suggesting that we leave it up there. What I am saying is

that if you just get one jurisdiction to prevent hosting, you will find that another of the 202 countries of the world will be hosting it.

Susie Hargreaves: I realise that is a problem but I do not accept that is not a reason to try to tackle it. The companies who host it are not the household names. There are a couple of bad actors based in the Netherlands that host this content. They are not the household names so they will not necessarily be covered by the Bill. Having said that, I think everyone in other countries is watching the Bill, so we need to get it right here and set the example.

Q46 **Chair:** Okay. Andy, where does age assurance stop and age verification begin, from your perspective?

Andy Burrows: Age assurance is clearly going to be crucial to this regime. It does so much of the heavy lifting. Our sense is that we support explicit age verification for commercial pornography sites, as we previously would have seen under the Digital Economy Act if that had been enacted, and for high-risk sites such as dating sites. Age assurance feels like the appropriate solution for social networks and gaming services. We are at a point where age assurance will be doing lots of the heavy lifting, as I say, in this legislation but we are looking at technology that is not in its infancy but is still actively developing. We have seen in the last couple of weeks guidance from the Information Commissioner's Office and its opinion on what compliance looks like under the children's code.

It is an area where, as this legislation receives scrutiny from the House, we need to have a much greater understanding of what age assurance techniques look like, and some clarity from Government and regulators about the thresholds. The technical solutions to achieve 99% confidence versus 90% confidence that a user is likely to be a child may be very different. There is a range of issues and trade-offs that flow out from that: for example privacy implications; are we talking about the use of biometrics versus a background analysis of content to determine if the user is likely to be a child?

We need to understand much more here and in time we should have a clear set of standards about what high-quality age assurance looks like. We have been in a holding pattern for the last 12 or 18 months where we have not seen a huge amount of guidance from Ofcom and the ICO. I have sympathy for the companies who have been working through what compliance looks like in the first instance with the children's code where we have not seen that clarity so far, but it is vital that we see that during this Bill.

Q47 **Chair:** Do you see it being effectively the parameters being upped as a result of this legislation above and beyond what the children's code has already set up?

Andy Burrows: I think what the ICO set out in its draft opinion a couple of weeks ago, which effectively would require high-quality age assurance

for high-risk services, feels about the right balance. It is vital that we have high-quality age assurance. Take a platform like Twitter, for example, where we know that there are significant problems with the platform hosting very age-inappropriate, sexually explicit material. There is a link here to sites like OnlyFans where creators are using sites like Twitter and TikTok to host promo content that is readily accessible to children and then can be recommended through algorithms.

We will need to have a high level of certainty. I think that is possible because, to put this very crudely, there is a reason that children receive adverts for computer games and not car insurance, but we need to have a sense of what standards and expectations are in place. We are somewhat operating in a blind until we have that clarity.

Q48 **Steve Brine:** Susie, COP26 is a big deal. The UK is responsible for about 2% of global emissions, so it is important that we lead by example, not least because we are chairing it, but at the end of the day if China and India and Russia don't come round the table then our leading by example will be just that. It won't achieve the ends, will it? Is the success or otherwise of this legislation dependent on a COP of nations in this space? Realistically, when we sit here in five years' time, what will have changed? What is the COP of this business? Is that a silly question?

Susie Hargreaves: No. I know exactly what you are saying. I think you are making a really interesting point because particularly online there is the global dimension, so how we all step up and deal with it is absolutely essential. There are provisions within this Bill to make children safer in the UK and it is not just that it will not have any effect unless everybody in the world steps up. I think it is good that these mechanisms are being put in place, that regulation is being put in place for the companies, and I think it means everyone will step up to a new level. There will be a level of accountability, which has to be a good thing.

As I say, the rest of the world is watching. We already have interesting mechanisms in Australia and other places, but it will provide a safer environment for children in the UK. For example, we have seen a 77% rise this year alone in self-generated content. This is children themselves in bedrooms and domestic settings who are being exploited, coerced into and filmed performing sexual activities that is finding its way on to child sexual abuse websites. We need the Online Safety Bill to make sure that we have the mechanisms to get the messaging out to keep those children safe online.

We run a project with the NSPCC called Report Remove, in the UK alone at the moment, that enables children to self-refer nude images of themselves without fear of criminalisation, for us to work together on safeguarding and having those images removed. We are being watched by the rest of the world on that and the States and Australia are going to put their own mechanisms in place. Somebody has to take the lead and it is important that we do that.

Q49 **Steve Brine:** Let me put it this way, if the rest of the world is watching, what are they making? I have been an MP for 11 years and I Google internet legends going into schools and telling young people about the dangers online and respecting their bodies, and yet you just told me that it is incredibly increasing. In the same way as MPs get very upset about people being rude and angry and abusive to us on social media, really they are just using social media as a means to do it. There is a sickness out there that thinks that it is okay to speak to us the way they do, but there is also a sickness out there that thinks that it is okay to view inappropriate images. Are we in danger of shooting the messenger here?

Susie Hargreaves: No.

Steve Brine: What is the root cause then? If there is a sickness in society that is doing this, the online environment is merely a reflection of the society that it serves, isn't it?

Susie Hargreaves: The internet is not all bad, is it? The internet has good and bad within it and it is important to recognise that, but you are absolutely right that now we have a situation where we have some really bad stuff happening. As with so many issues, if you just thought that then—for me, if we take down one image a day that stops a child being revictimised. We take down thousands of images a day and we have to do it for those children and we have to start somewhere. Yes, it is a war of attrition, and maybe we have to do it an image at a time, but we also need the influence, the legislation.

There are three ways to tackle child sexual abuse. You cannot do it through legislation alone. You have legislation, law enforcement effort, the technology to fight it—and we need to hold the technology companies to account to create new technology all the time—and the third is through education and awareness. Those three pillars all need to be put in place in every country. We are working with other countries to help them build their capacity to fight this issue. I agree with you that you could just say, "What is the point? It is a needle in a haystack", but we have 21 analysts looking at child sexual abuse every day and they go home knowing that they took down images of children being sexually abused. You have to start somewhere.

Q50 **Steve Brine:** It is a war of attrition. Is it a war that we are winning?

Susie Hargreaves: I think we are winning on some fronts. That is reality and on some fronts we have a hell of a fight ahead of us.

Q51 **John Nicolson:** Thank you both for joining us today. Let's talk about Facebook. It is in everybody's minds at the moment, I think, and most of us will have read yesterday's *Times* with the story that 24 children a week are groomed on Facebook. Mr Burrows, can you tell us why that happens and what makes Facebook and Instagram especially pernicious?

Andy Burrows: Facebook-owned apps account for more than half of grooming offences. This is the offence of sexual communication with a

child in England and Wales. In part that is the product of Facebook doing something well, which is that it accounts for the vast majority of child abuse reports and other parts of the sector lag behind in their reporting capacity. But this is also very much about Facebook's culture and design decisions that have not had child safety as a primary consideration far too often.

Q52 **John Nicolson:** Not as a consideration at all because we know that large numbers of 10 year-olds are using Instagram. They are not meant to be using Instagram. They are being groomed on Instagram; they are obsessing about the way they look on Instagram; they are being bullied at home on Instagram and they are 10 years of age. It is outrageous that children of 10 are on Instagram and facing these kinds of dangers without Facebook coming up with any solutions.

Andy Burrows: Let's be clear, far too often Facebook's response to child safety concerns has been driven by a PR strategy and looking to attempt a media rebuttal rather than rolling up their sleeves and making sure that the sites are fundamentally safe for children. If we look into that grooming data in more detail, we can see that Instagram has increased the total number of offences on Instagram during the four years since this came on to the charge sheet but also as a proportion of offences. We have not seen action being taken that is in any way commensurate to the scale of harm that children are being exposed to.

John Nicolson: Right, so Facebook is enabling grooming?

Andy Burrows: Facebook is failing to take design choices that reflect the scale of harm on its sites.

Q53 **John Nicolson:** I think that is a gentler way of saying what I am saying. Ms Hargreaves, what can Facebook do to address this crisis that it has that it is a grooming enabler? Let's call it what it is.

Susie Hargreaves: Facebook is one of our members. We work closely with Facebook. We are funded by the internet members and it is one of our top tier members. I am going to give Facebook some credit that it has a committed team of online safety people in the organisation who we work very closely with. It funds a number of additional projects and provides us with engineering support.

Q54 **John Nicolson:** Wait a second. Nobody doubts that there are good people working in Facebook—that goes without saying. There will be good people who work in Facebook, but Facebook as a company is doing something that is fundamentally evil, which is allowing 10 year-olds on to Instagram where they get groomed and abused and bullied, and it is doing very little to prevent that from happening.

Susie Hargreaves: I think we would all love to hear Mark Zuckerberg say that issues like child safety are as important to him as privacy and shareholder value.

John Nicolson: Of course we would but he is hiding away in California and he is too scared to come before this Committee.

Susie Hargreaves: For the IWF specifically, bearing in mind we are dealing with images and videos, to provide balance to what I said originally, on the one hand it is doing some really interesting work with us and on the other hand it has plans to encrypt Messenger. Encrypting Messenger will have catastrophic effects for the ability of Facebook to identify child sexual abuse images.

Q55 **John Nicolson:** Mr Burrows, Facebook and Instagram are bad enough here in the United Kingdom but we see them at their best in the United Kingdom because we all speak English and the English language is where they put in most of their attempts at very ineffective control. We know that throughout the world, in 99% of languages spoken around the world, there is zero moderation at all. If you are a child in Turkey or Greece or Afghanistan or Syria or a hundred other countries, you can be groomed and abused without any moderation whatsoever.

Andy Burrows: We heard from Frances Haugen who said precisely that just yesterday. I think there were figures about misinformation provided in part of the data dump yesterday that suggested 87% of the activity was focused in the United States. I think that is a real issue.

What this boils down to is corporate culture. It is very clear that in the absence of regulatory drivers so far and in the absence of commercial drivers that have been enough to focus minds, children's safety in the UK or around the world is secondary. It will be secondary for Facebook in particular every time that there is a trade-off to make if we are talking about children's safety versus privacy benefits for the rest of us. If we are talking about the balance between privacy and safety and a range of fundamental rights, children will lose every time. I think it speaks to issues about the corporate culture in Facebook that time and again we see children on the losing end of those trade-offs. I don't see how that will change unless and until we see effective regulation here in the UK. To go back to the point earlier, if we do this correctly in the UK it can be a precedent for how we do this internationally.

Q56 **John Nicolson:** What is breadcrumbing?

Andy Burrows: Breadcrumbing is where we can see activity that in itself will not meet the criminal threshold for removal but where we see abusers posting that content on social networks, often with a clear sense of how they can game content moderation rules. They know what they can post and what they cannot. This could be tribute sites, pictures of a child that to you and me would be perfectly innocuous but if you are an abuser you will recognise the context behind it. These are carefully edited child abuse sequences, so they are edited in such a way that they are on the right side of what platforms will keep up rather than take down. They effectively allow child abusers to use platforms as an online shop window to advertise their sexual interest in children and then in turn to form

networks that will go off platform to encrypted sites, to less scrupulous platforms where abuse material can be shared.

As it stands in this Bill we are concerned about whether that content will be actioned and that is a product of the Bill having the separate buckets between illegal and legal activity. There is a risk that this falls into a grey area where it is not captured because it is not legal content.

Q57 **John Nicolson:** This is repulsive, the image of breadcrumbing. It is a paedophile, an abuser who is dropping breadcrumbs to lure children away from a place that we already know is dangerous but at least has a modicum of protections or pretend protections. At least we know the name of the site, and it is dropping these breadcrumbs to lure a child away from that into a world where there are no controls of any kind, the kind of world where Afghan children live all the time on Instagram, a world without protection and monitoring.

Andy Burrows: It is activity that directly facilitates abuse and that is why we think it is important that the safety duty should be flexed so that this is addressed. If we are not addressing those types of risks, the legislation is not being as proactive and upstream as it needs to be.

Q58 **John Nicolson:** Ms Hargreaves, I do not know whether or not you have children, but if you had a young teenage child would you allow him or her to use Instagram?

Susie Hargreaves: I do have children, quite old children, and my daughter uses Instagram but she is in her 20s. As a director of the Safer Internet Centre I think that the key responsibility for us is to ensure that children have the mechanisms to keep themselves safe online. That is not to negate—

John Nicolson: You can't at 10.

Susie Hargreaves: No, absolutely, which is why we have been talking about having age assurances and appropriate mechanisms—

John Nicolson: Or 12 or 14.

Susie Hargreaves: I agree with you on that. I think you can at 14 if you have the right support and education, the right safety mechanisms in place. It is not a question of yes or no; it is a question of ensuring that we have those protections in place.

Q59 **John Nicolson:** Mr Burrows, the same question: would you allow a young child on to Instagram? We are in a peculiar place here, aren't we, because we have no experience of this? We don't have any idea at all what this is going to do to the brain of a 10-year-old because we are in uncharted territories. I am guessing that for a 10-year-old who grows up in this bullying environment, a 10-year-old, a 12-year-old, a 14-year-old who is bullied at school, bullied on the way home, bullied at home and then goes to sleep at night and the last thing they see is bullying and the first thing they see in the morning is bullying, it will have a pretty dire,

disastrous consequence on the development of that child as he or she grows to maturity.

Andy Burrows: It is a real dilemma for parents up and down the country. I was having this conversation with friends at the weekend. Clearly we know that the majority of children under 13 are on social networks and children themselves will be clamouring to get on to these sites. Very often children are using the sites not just for entertainment or to post messages but also as a means of communication. Children use Instagram in a way that, for example, we might use WhatsApp to communicate. It is a very difficult situation right now because too many of the sites in too many respects are not fundamentally safe by design. I think the regulation can ensure that we have fundamentally safer products but this has to be about the onus being on the tech firms to ensure the platforms are safe by design and that we have a parity of protection between children's physical worlds and their online worlds.

Q60 **John Nicolson:** To be absolutely clear, this Bill as it currently stands does not do what you want?

Andy Burrows: It needs to be much more ambitious if it is going to meet that target, yes.

Q61 **Giles Watling:** I think we all agree that we are trying to get the platforms to take responsibility, but on the back of the answers that you were giving to Steve Brine earlier I would like to ask you—I looked at the Internet Watch Foundation. You have around 160 members who support you and they include Twitter, Facebook and so on. Is this a case of keeping your enemies closer, because don't you find there is a conflict of interest there?

Susie Hargreaves: Thanks for that question. We were set up by the internet industry on the principle that they would clean up their own networks. We now have 171 members, some of the biggest companies in the world. The principle that we work to is that we have to work with them, so we provide them with technical services to help disrupt the distribution of child sexual abuse and they pay for the hotline. We have always been free of Government funding. We have had occasional grants from the Government but we are being funded by the industry to clean up their own act.

I think the question on conflict is an interesting one. This is an interesting area and the Online Safety Bill will not work unless we work with the companies, so the regulation has to be done in partnership with the companies. We may be funded by them but we have lots of independent checks and balances. We have a majority independent board and an independent audit of our hotline. During the independent inquiry into child sexual abuse, our work was commended as being a successful element in keeping the internet safe of child sexual abuse in the UK. I get why people say, "You work with the industry, you are conflicted" or whatever, but the reality is we have to work with them to get rid of this

content and we ensure that we put as many checks and balances in place as we possibly can.

Q62 **Giles Watling:** But it all comes down to money, doesn't it? This is what these companies do. This is why they don't want their models interrupted and fundamentally you are paid for by these companies. It is certainly, to my mind, a conflict of interest. How do you answer that? We as MPs around this table are all lobbied and I imagine you are lobbied by the very people who provide your financing.

Susie Hargreaves: No, we are not, actually. If the companies don't pay to clean up their own networks, the taxpayer would and I think it is fairer that they pay to have their networks cleaned up. One of the things that we can evidence again and again is that while we are funded by the internet industry, we do not always take a stance with them. The issue of Facebook is a really good one where we are absolutely side by side with the child protection organisations on opposing Facebook's introduction of encryption on Messenger without it having appropriate safety mechanisms in place. We are quite happy to publicly speak about that and where we feel that they are not taking a child protection stance on child sexual abuse we will take a stand.

The other side of it is that we have masses of conversations behind the scenes with members. We work with them, so we say that we have identified a problem and we work with them to ensure that we get the services and the mechanisms in place to help clean up their act. We benefit from engineering support. We have had engineers from Google and Microsoft. We run a number of projects where we get their technical expertise to help us fight the problem. That partnership is absolutely critical to ridding the internet of child sexual abuse. My personal view is that they should pay for it, not the taxpayer.

Q63 **Giles Watling:** I agree with you on that. I wonder whether this working with them is working for you, that you can say absolutely clearly here at this Committee that you are independent of those people who provide you with finance.

Susie Hargreaves: I think our track record speaks for itself. We have a world class reputation. Last year we provided about 60% of the European database on child sexual abuse. What we have shown is that partnership is key, whether that is law enforcement. It is a very complex issue but the majority of the companies we work with are American and they have Fourth Amendment issues in working with an agent of the state. We provide this air gap brokering position where they can take our data and our services and deploy them across their platforms without there being any conflict for them in working with agents of the state. That is an important brokering relationship that we need to have and it is essential if we are going to try to fight the problem globally.

Q64 **Giles Watling:** Thank you for that. I would like to move on to freedom of speech, because it is at the core of our democracy, as we all know. I

know, Andy, that you are calling for a general duty of care in this Bill. Is it possible to have a general duty of care that does not trample over freedom of expression?

Andy Burrows: I think it is absolutely possible. How we envisage an overarching duty of care is that it is a requirement on platforms to take reasonable and proportionate steps in the design of their sites and in how they are run, to identify and take reasonable action on safety risks, overseen by Ofcom as a regulator who can bring a track record in dealing with issues of freedom of expression and of balancing the range of fundamental rights at stake. I make no bones about the fact that this is a very difficult piece of legislation to land effectively the balance between free expression and privacy and safety. These are not new issues and they require very careful thought to land them correctly.

The reason I think that legislation is so important is that we have seen that the product decisions will not land at the right balance in and of themselves. Susie mentioned end-to-end encryption, which has very clear benefits for privacy and free expression and participation, but to unlock those in a safe and responsible way we would expect that a platform like Facebook is building technical mitigations to ensure that that does not put a wrecking ball through child safety. At a stroke, unless those mitigations are in place, 70% of child abuse reports will be eliminated at the flick of a switch.

These are very difficult balances to get right, I make no bones about that, but I feel much more confident that with a well designed regulatory regime, and a regulator with a track record and expertise that Ofcom brings to this, we can expect to have a better balance than we are seeing the tech firms arrive at in decisions relating to children right now.

Q65 **Giles Watling:** But you really believe that we can preserve freedom of speech?

Andy Burrows: I think that we can, absolutely. There are measures in the draft Bill that will, for example, extend super complaint powers to bodies representing freedom of expression and also privacy concerns. There is the checking clause in the Bill to maintain freedom of expression. I think it is important that we recognise that freedom of expression and freedom of reach are different things and that we recognise freedom of expression as being the right to participate. Very often lots of those safety trade-offs are not landing in the right place now and we are seeing users who don't feel able to exercise and participate on social networks in the way that we might like. I think that we can get there but I do not underestimate the challenge for Ofcom in doing this effectively.

Q66 **Alex Davies-Jones:** Thank you to our witnesses for joining us this morning. You have both outlined some of the most urgent and prevalent harms facing our children on the internet at present. Have these been exacerbated by the pandemic?

Andy Burrows: I would say absolutely. Our assessment is that the pandemic has been probably the greatest single period of risk for children in child abuse in particular that we have seen. Our concern here is that this is not necessarily an issue that is in the rear-view mirror as, hopefully, we are starting to move beyond the worst of the pandemic. There is a reasonable sense that the structural threats as we emerge out of the pandemic may have changed. To give a couple of examples of what I mean by that, let's think about how children are now using livestreaming and video site services, as we all are much more frequently than before the pandemic. Those are high risk sites for children. If you think about a child who is being groomed, the live, inherently visual nature of those platforms is incredibly high risk. It requires a set of design mitigations that we do not see most of the platforms having in place and during the pandemic we saw platforms look to rush out products in a chase for market share before mitigations were in place. If we are now talking about children using higher risk functionality that is going to be a longer-term change to the threat.

Similarly if, for example, we see a long-term shift in working patterns and greater degrees of home working, if we are talking about abusers looking to access images and they are not in an office in a more structured environment, that is likely to have an impact on the demand for images and in turn probably on grooming to fuel it. It has been a period of considerable risk and we do not necessarily return to the base that we were at in March 2020, unfortunately.

Q67 **Alex Davies-Jones:** Are any of the harms that you have both mentioned already currently not covered by the provisions in the Bill? Is there anything that should be added as a priority to ensure that they are?

Susie Hargreaves: We are dealing with illegal content. We need to ensure that it is principle based and that we are not too prescriptive within the Bill so that we can adapt to deal with technology as it changes. From our perspective, no. We would like to see age verification for adult sites as a real priority and that is not covered in the Bill. We know that people access adult sites as a pathway to child sexual abuse, so we want to be able to work with the adult providers to provide technical services but we cannot do that without age verification being in place. We need to ensure that that is addressed within the Bill, but overall I think the problem at the moment is that there are so many harms covered. The devil is in the detail here and how it plays out in secondary legislation is the issue for us.

Andy Burrows: To pick up on that, it would be beneficial as the Bill goes through to have greater clarity on which harms are in scope. It is understandable that some of this will come back through secondary legislation, but it means that that is a real challenge in effective scrutiny when we do not necessarily know which harms will be identified as priority harms or not. There are parallel activities in play. The Law Commission has proposed new communications offences and how that

might extend to cover suicide and self-harm content, for example. That is running in parallel and it would be optimal if we could see the Government clarify their intentions as to whether those will be brought forward. As it stands, I don't think any of us, including Ofcom, know what will fall into the bucket of legal and what will fall into harmful and, therefore, what the shape of the regime will look like.

Susie Hargreaves: The priority content needs clarification, particularly for the lawful but awful images. The IWF often find that we have a series of images where we cannot take action on a number of them because they do not meet the legal threshold. The projects when we are working with NSPCC where a young person can self-refer an image of themselves at the moment might not meet our legal threshold but might be causing them real distress, so it is having the ability to remove that. There is a number of cases where the priority content on the margins of what is illegal need to clarified.

Q68 **Clive Efford:** A lot of what I was going to ask has been covered, but I will plough on. The threshold for both primary priority content and priority content that is harmful to children will be designated in regulations by the Secretary of State. Is that the right approach?

Andy Burrows: I think it would be beneficial to have clarity during the scrutiny process as to which harms are minded to be in scope. There may be mechanisms that would be beneficial for parliamentary scrutiny rather than just getting to the point where there is a piece of secondary legislation after this has been developed. It would be beneficial to have that clarity so that we can understand what the scope of the regime will look like. There is clearly a difficult tension here between Ofcom needing the time and space to build its risk profile as set out in the Bill and then to understand which harms should be in scope. The challenge is that because so much of the Bill is effectively a scaffold for the secondary legislation, the codes and the guidance that will flow through, there is so much that we cannot pin down at this stage.

Susie Hargreaves: I agree. On the issue of the Secretary of State, you have to ask about the independence of the regulator. We want to ensure that decisions are made with careful thought and an understanding of the context in which they operate. For example, there might be an issue about something that is not technically possible or might have perverse consequences because it is not thought through properly, so we want to see what that looks like in secondary legislation.

Q69 **Clive Efford:** Is there an issue around what content could be designated as harmful to children but simply could not be labelled as illegal content?

Susie Hargreaves: I think that is a big challenge. We only deal with illegal, as I have said many times now, but there are lots of areas where we need that clarification. The issue for us is that on one level it is easy because we have clarity in law. We look at an image: is it illegal, is it not

illegal; we remove it. The issue about harmful content is it becomes so much more complex and that is very much in your area, isn't it, Andy?

Andy Burrows: Yes, absolutely. I think there is an issue here about the way in which technology and market changes in the next few years will change the nature of the threats. We are expecting later this week, for example, that Mark Zuckerberg will make an announcement about the move towards a metaverse. It is very difficult right now to understand technically what that will look like as an end product, but if we play that at face value where we are talking about an immersive experience in which harms potentially can be felt and experienced, not just that a child is subject to, that has very significant implications for how we might want to mitigate harms, what that means for the regulation and potentially what that means for the legal landscape as well. Do we start to see a blurring of what we might consider right now offline and online abuse in separate buckets? One of the challenges with the differentiation between legal and illegal forms of content, in the absence of an overarching safety duty that helps to focus the legislation around core safety objectives, is how well this could all be future-proofed for where we might be in, say, five years' time.

Q70 **Clive Efford:** One last issue, which was touched on by John Nicolson earlier on, is the evidence of Frances Haugen to the Select Committee. We tend to talk about this as exploitation of children by adults but a number of reports have pointed out bullying and interaction of children on Instagram, which she referred to specifically yesterday. In the Ofsted report in June an astonishing number of young women were saying that they had experienced online abuse from peers, boys but boys of their own age. This is a learnt experience that is the starting point that will lead later on to abuse such as violence against women and girls. Do you think this legislation is an opportunity to get to the root of that or does that need some separate, specific measures to deal with it? I want to give you the opportunity to comment on it.

Andy Burrows: We can make great strides with this legislation. On illegal content, we know that about 80% of sexual communication with a child offences take place against girls and similarly the harmful content disproportionately affects girls as well. I know that will be the theme of the next session. What we can reasonably expect through this legislation is a requirement on platforms to take design choices that can help to mitigate some of the worst effects of that, making sure that platforms are a safer experience. An example is self-generated images and steps that can be taken to frustrate the share and the spread of those to empower young children to have content removed that is upsetting to them. This piece of legislation is not the only answer to a very complex set of issues around peer-on-peer abuse but we can certainly expect and hope that we can make great strides with it.

Susie Hargreaves: I agree with Andy on that. It all comes down to the clarification. We have an issue at the moment that it is really difficult for

children to prove they are under 18 in this country. On our Report Remove project we have a situation where a child has to provide some evidence that they are under 18 for us to remove their images and that clearly cannot be right when we have a situation where children have images in circulation that distress them. There are all sorts of things that we need to look at, but it comes down to the detail.

Q71 **Chair:** Andy, just on one point before I turn to Julie, should the Bill be presented with draft regulations in place in your sphere in relation to child sexual exploitation to allow MPs to better understand what is intended? It seems to me that we are just going to be signing off immense powers to the Secretary of State without gauging what that means in practice.

Andy Burrows: I think parliamentary scrutiny of some of this detail will be helpful, because it is practically difficult right now. The nature of this Bill is it is enabling this complex flow-through of secondary legislation of codes, of guidance. I think we do need to see more detail to gauge the overall effectiveness.

Q72 **Chair:** That is a yes; you believe that the Government should publish alongside the draft Bill at Second Reading these regulations in order that we can check them out and see that they do what we want them to do?

Andy Burrows: That is one way of doing it. There are other mechanisms. There can be forms of scrutiny as Ofcom goes away and develops its risk profile. There are other options there that can be explored. Certainly I think the ability to scrutinise the legislation effectively is important.

Q73 **Chair:** So is five days enough time?

Andy Burrows: I struggle to see how five days, even with a plentiful supply of coffee for this Committee, is enough. It is very challenging.

Chair: We do get through a lot of coffee, Andy, at least in my case. Thank you. I get the point.

Q74 **Julie Elliott:** Good morning. We have heard a lot about age assurance systems this morning. Are they the only way to assess whether a service is likely to be accessed by children or are there other practical alternatives to age assurance systems?

Andy Burrows: I think age assurance is the most logical way to be able to determine if a user is a child. Age assurance potentially covers quite a wide bracket of solutions. This could be, on the one hand, the use of biometrics to determine if a user is a child; it could be through an analysis and understanding of the content that they are using. It could also be measures to couple a device with that of a parent or a guardian, so there is that offline—

Q75 **Julie Elliott:** Should the Bill be more specific about the requirements of age assurance?

Andy Burrows: I think we need to have more clarity on that, yes. As I suggested earlier, age assurance is going to do a lot of heavy lifting in this Bill and, because it is still a nascent set of technologies and set of solutions, then we need to have a clear sense of standards but also an expectation of what the outcome is. Is this age assurance with 100% certainty or 90% certainty? How you arrive at those thresholds of confidence will have significant implications for how companies may go on and do this.

Q76 **Julie Elliott:** Do you think age assurance is going to work?

Andy Burrows: We need certainty about what the technology is able to achieve. My sense is that this is a practical way forward because I think for some of the larger platforms they clearly have a very good micro-targeted understanding of who their users are. This is something that can be delivered but we must have greater certainty on that because it does so much of the heavy lifting for the legislation. We need to hear from Government if there are aspects of age assurance that may not deliver in the ways that they require or how else they would arrive at some of the legislative objectives.

Susie Hargreaves: I want to add it is essential that we look at tightening up age assurance, but to echo what Frances Haugen was saying yesterday, that we need to have more transparency from the companies in relation to what they are doing to ensure that children are the right age to be on their platforms. At the same time, I also think that it is absolutely essential to say that it is not really simple. There is not any technology in the world now that can accurately age a child 100%, but there is a sense that technology companies can just resolve it immediately, tomorrow, with some kind of technology. It is complex, but there are lots of things that are complex in terms of technology and that should not stop us doing it. We are always looking at new ways to innovate and create new things.

I would also say two things, that there is absolutely no excuse for there not being age verification on adult websites because then we are talking about adults, and the second thing is that no one should have access, regardless of their age, to illegal content.

Q77 **Julie Elliott:** I was going to ask a supplementary to my organised questions about age verification on adult sites and at some point you talked about commercial pornography sites. I absolutely agree there needs to be age verification in this Bill for that, but what about self-generated sites, because they are just as damaging? Do you think age verification for self-generated adult sites should be there as well?

Susie Hargreaves: I think wherever you have adult content there should be age verification in relation to people having access to that material. We have a different reason for wanting to work with adult sites, because where the content is legal, regardless of what you might personally think about it, those are pathways to child sexual abuse. We

want to be able to deploy our services across those sites. It is essential that we do get proper age verification on adult sites. Andy can probably speak more to those platforms.

Andy Burrows: One thing I would say in respect of pornography is clearly we need to see the legislation close the gap where this Bill will achieve less than the Digital Economy Act would have done if that had been enacted. This is about making sure that the scope of the legislation tackles pornographic content, but also about the child use test in the Bill. We have a concern right now in respect of pornography but potentially in terms of other forms of age-inappropriate content as well, that the threshold for the child safety duty appears to be higher than applies in the Children's Code. Whereas the Children's Code determines if a site is likely to be used by a child then it is in scope and then it has the risk-based approach to enforcement to ensure proportionality, here there is a higher threshold. So a platform would only be in scope if there is a significant proportion and/or number of child users. That presents a scenario where you could see a site like OnlyFans legitimately able to argue that it is not covered as it is currently drafted by the child safety duties. I think that is a drafting issue that needs to be closed, because otherwise the risk is that we are not preventing harm and access to inappropriate content, but are simply displacing it.

Q78 **Julie Elliott:** It needs to be clearer, and more capturing is the gist of what you are saying. Would you agree with that?

Andy Burrows: Absolutely.

Q79 **Julie Elliott:** One of the things we have been told is that the inclusion of age assurance systems would be bad on privacy grounds for users and economic grounds for service providers, particularly start-ups. How would you both respond to that comment?

Susie Hargreaves: Again, in relation to illegal content, it is complex. We echo what the NCA's position is, that we are able to identify a lot of bad actors, so we want to ensure that we track and follow them. There are reasons why children might need anonymity, so it is complex but again we think we need to have clarification in the Bill and some very clear framework and guidelines around that.

Andy Burrows: For us, the importance of standards is crucial. For example, some of the biometric routes to achieve age assurance will raise issues of privacy that need to be worked through and will benefit from parliamentary scrutiny and from civil society debate. The objective here should be moving towards standards and we need to have the clarity of what is expected and therefore what the routes to achieve that will look like, so that we can then start to have that conversation around specific proposals.

I think it is a fair point, and this applies in terms of age assurance, but it applies in terms of the regulation across the piece that we need to ensure

that the costs of compliance are reasonable, so that we are not introducing barriers to competition, so that this does not penalise start-ups, and I think there is a strand there for the regulator and for DCMS about non-legislative solutions. DCMS is doing some excellent work in respect of the safety tech market, so we might be talking here about white label plugin solutions that platforms can use if they do not have the economies of scale and scope to develop their own solutions. It is important that we see that work continuing apace.

Susie Hargreaves: If I could add there, the whole issue of safety by design is in a different place now to where it was 10 years ago. Half of the problems that we are dealing with are because these companies, which are now massive, did not have safety by design and they suddenly realise they have a safety problem. The fact that DCMS are focusing on that and providing support for start-ups to ensure that they can build in some safety by design is essential.

Q80 **Chair:** Susie, to pick up on one point there, you said that age verification should be required for access to adult materials or sites that carry adult material. Should that be adult sites or sites that carry adult material? Of course Twitter carries, as we have already heard, a huge amount of adult material. Is it just for Pornhub or is it just for Twitter that we have age verification?

Susie Hargreaves: That is a really good question.

Q81 **Chair:** Hopefully without displaying too much personal knowledge.

Susie Hargreaves: The issue around Twitter is it falls under the age barrier of social media. We know that there is an issue there. Twitter was looked at as part of the Digital Economy Act and with the proportion of adult content it was not deemed to fall under the remit of the Digital Economy Act. I do not have an answer on that, because my focus at the moment is on the mainstream adult sites, Pornhub, the big ones.

Q82 **Chair:** If you use one of these websites, now obviously the Digital Economy Act had the I think farcical notion of going down to your local newsagent and taking your ID with you and proving who you were, if you were able to find a local newsagent, of course. What happens to your ID if you upload it to one of these adult sites? Are we trusting people's ID to individuals who host such material? Is that a good idea?

Susie Hargreaves: The mechanism for doing that is not my expertise, but we do know if you look at many financial sites, and gambling there are loads of mechanisms in place that could be replicated. There are lots of ways that people can verify their age without a new third party-type situation. We currently have that on Report Remove, with an age verification organisation called YOTI. This is for people to verify that they are under 18 and where they submit a passport or identification that is verified by an independent body.

Q83 **Chair:** It gives you a passkey, therefore?

Susie Hargreaves: Yes, there are lots of ways to do that but that is not my area of expertise.

Q84 **Chair:** Better than a newsagent, no doubt.

Susie Hargreaves: I would have thought so.

Q85 **Kevin Brennan:** To follow up on that, age verification was legislated for under the Digital Economy Act and many of us on the Committee did warn how impractical it was within that Act. Of course, ultimately the Government chose not to bring that into force. Why do you think it failed last time around when the Government tried to do this?

Andy Burrows: One thing that we can say, in terms of the issue about practicality, there were lots of concerns raised about the privacy implications and the way in which data of users could be put together. My understanding of this is that there are a range of providers that are ready to go, which are third party providers and what—

Q86 **Kevin Brennan:** In fairness, that was previously the case. That argument was used during the Digital Economy Act, that there were plenty of third party providers, but the Government dropped it ultimately. Why do you think they dropped it?

Andy Burrows: There were clearly a lot of concerns that were not being effectively answered about privacy risks that were being put forward, which I do not think stands up against some of the solutions that were in—

Q87 **Kevin Brennan:** Do not get me wrong, I want to see a comprehensive Online Safety Bill, but there is always a danger with this kind of legislation and you spoke earlier on, Ms Hargreaves, about Christmas tree Bills. The danger with this kind of Bill is mission creep. Is it not the case that if this becomes, and there may be a case for it, a Bill about stretching what is outlawed as adult content that is currently on those sorts of sites, stretching the illegality definition of that to bring it in line with the NC-18 rating on physical adult content, that once you start going down that road you are losing focus on the essence of what the Bill should be about, which is online harms, protecting children, and getting into an area that is a very important area, but which should be the subject of a wholly different piece of legislation if you want to tackle the content that is currently available on those adult sites and is currently legal, whatever you think about it. You are going down that road. Is there a danger that is what is happening here, or am I wrong?

Susie Hargreaves: No, I think there is a danger, but it is also an Online Safety Bill, so children are accessing adult content, so that has to be addressed in order for them to be safe.

Q88 **Kevin Brennan:** The point I am making is that it became an issue not of age verification in that Bill; it also became an issue partly because of the involvement of the British Board of Film Classification in the definition of

what would be legal content, it became an issue and this is a separate issue in my opinion, of banning particular content that is currently available and currently deemed legal.

Susie Hargreaves: I do not know. I do not think I know enough to go through why it failed but we need to deal with the situation now. You could argue exactly the same thing about privacy or whatever, that there are lots of considerations to think about in relation to online safety, but ultimately we want to make the internet safer for children. I think we must go back to those fundamental principles. We do know that the biggest adult provider is prepared to work with organisations to get age verification in place. I think these things have to be tackled in whatever way they can and the danger is if it is too detailed and prescriptive we are going to have all sorts of problems within this Bill.

Q89 **Kevin Brennan:** You said earlier there had been a 77% rise in self-generated content by children. Why has that happened and over what timescale?

Susie Hargreaves: On self-generated content, which we also now call self-produced content, we run the secretariat for the APPG on social media and we ran an inquiry recently into the rise in self-generated content. We started seeing it as an emerging threat in 2012 and it has risen year on year. We would put it down to a number of factors, so we know that over 92% of the children are girls and they are aged 11 to 13. They are on all sorts of different platforms. There are many ways for them to be tricked, coerced, encouraged, groomed into sharing sexual activities. By the time we see it, it has been captured, harvested—we do not see it in the original location—and put on a child sexual abuse website. We would say that Covid has played a massive part in that, so we have seen a huge increase—

Q90 **Kevin Brennan:** To be clear, the 77%, did you say that was since 2012 or since Covid?

Susie Hargreaves: We saw a 44% increase in 2020 and in 2021 so far, we work on a calendar year, we have seen a 77% increase on the year before.

Q91 **Kevin Brennan:** So 77% in the last calendar year and 44% on the one prior to that?

Susie Hargreaves: Yes.

Q92 **Kevin Brennan:** This is extraordinarily exponential growth in this kind of content. Do you remember the 10-year Byron report way back in the day when I was Children's Minister between 2007 and 2008 in the last Labour Government? Do you think the lessons of that report were learned in that period you have just talked about, 2012, and integrated into Government thinking?

Susie Hargreaves: I remember the report but I cannot remember the specifics around it, so I would not want to address those completely. It kickstarted a whole approach to—

Q93 **Kevin Brennan:** I agree it is ancient history, and we were talking about Bebo back then, which as far as I know no longer exists. The essential insight of the report, perhaps slightly to contradict my good friend and colleague John Nicolson, was that the really important part of all this is that yes, swimming pools are dangerous and you should put up a sign saying, "Swimming pool, deep end, dangerous" but what is more important is to teach children how to swim and to keep them safe.

I remember at the time talking to my own daughter who is now grown up but was making YouTube videos and had 80,000 views of these mashup videos and I said, "Let me have a look at the comments" and one of the comments said, "Your videos are very good. How old are you?" and she replied, "It's not my policy to reveal my age" and I thought, "Good girl".

You did talk about education earlier on. Has that not been a missing part of the puzzle that there has not been a national—I received a thing here from Google yesterday doing lovely things about educating your kids, find your balance hashtag and all that sort of thing, but why should that be being done piecemeal by your sponsors who by the way, I know it is better that the taxpayer does not pay for things, but if they paid their taxes then maybe they would be taxpayers and they could pay for it directly? Should there not be a proper, nationally organised education and information programme, rather than piecemeal initiatives by huge multinational companies?

Susie Hargreaves: Yes, because education is absolutely critical. I am also Director of the UK Safer Internet Centre and we run Safer Internet Day with partners Childnet International and South West Grid for Learning, who run awareness raising in schools and a helpline. There are many other organisations like the NSPCC and people who run online safety briefings. We are currently running a national campaign on targeting parents and carers, so, "Do you know who is in your child's bedroom?" around self-generated, and we are also doing one that is targeted at girls aged 11 to 13 to empower them, not to frighten them, but to empower them to take control, to block, report, tell someone you know, if someone asks you for a nude.

We need to get this message out. Picking up on the previous question, we cannot just ban the internet. It is a bit like saying we will ban cars or alcohol. We must deal with the situation we have and the education piece is crucial. One of the most shocking statistics about the rise in self-generated content is the fact that we are also seeing a huge increase in seven to 10 year-olds now, so we need to get the education message out as soon as possible. Yes, the internet companies should be paying for it. We are not there yet and we do not pretend we are.

Q94 **Kevin Brennan:** As you know there was a very long period of time

where that part of the education curriculum was never updated, but I will leave that point. Briefly, I will ask two things to Mr Burrows. First, you said earlier on and it staggered me when you said it, for Facebook you said that children's safety is secondary. Secondary to what?

Andy Burrows: When you look at the last decade or so in the absence of legislative or regulatory requirements to embed children's safety into decision-making, and in the absence of commercial motivations, then—

Q95 **Kevin Brennan:** That is a very long answer. Secondary to what? If you say a lack of commercial motive, do you mean secondary to profit? Is that what you are saying?

Andy Burrows: Yes, absolutely. What we have not seen is an investment in trust and safety to make products safe by design that matches the level of risk.

Q96 **Kevin Brennan:** Ultimately, from what you are saying, from the NSPCC, is that for Facebook children's safety is secondary and it is secondary to profit. Does that not suggest a moral failure on a monumental scale by that corporation?

Andy Burrows: Too often when we and others have had discussions with Facebook, where we have published data on the scale and extent of the growing threat of child sexual abuse, the approach has been to try to dismiss that as a bad news cycle.

Q97 **Kevin Brennan:** Is that moral failure on a monumental scale?

Andy Burrows: I think it raises significant questions about the culture.

Q98 **Kevin Brennan:** NSPCC cannot say that that is a failure on a monumental scale?

Andy Burrows: It raises significant questions about Mark Zuckerberg and the leadership team that have failed to recognise that there is a clear responsibility to protect children, and it should not just be seen through a compliance lens.

Q99 **Kevin Brennan:** You are not going to let me put those words in your mouth. Should we take evidence from children and young people in our inquiry, and, if so, how can we do it safely?

Andy Burrows: I think absolutely children and young people should be able to give evidence. I am sure we and other organisations would be pleased to support this. If I may, I would also say I would like to see Mark Zuckerberg give evidence to this Committee.

Kevin Brennan: You may not know this, but last year when they sent someone along and I asked them if they had ever met Mark Zuckerberg, the witness they had sent along had never met him, although he had seen him in a room. Neither had he ever met Nick Clegg. If you want to know what Facebook thinks about the UK Parliament, there is your answer.

Q100 **Simon Jupp:** Good morning. Let us get geeky for a second, if we may. Obviously, any Bill or legislation that is put forward needs to be future-proofed. How future-proofed do you think this legislation is at the moment? I am particularly thinking about VPNs and all sorts of new, existing and emerging technologies that can bypass any of the safety precautions put in place by this Bill.

Andy Burrows: I think we do have questions about whether the legislation as it is drafted is sufficiently future-proofed. A couple of points that I would touch on. The proposed use of technology warning notices places a Catch-22 on Ofcom that to use those notices it must demonstrate a persistent and prevalent problem when some of the measures that we will be looking to act against take away the capacity to be able to prove that. I do not see how that is resolvable in how the Bill is currently drafted.

Another area where I struggle to see that the legislation is future-proofed as it stands is around the move towards decentralised social networks. We know that Twitter, for example, has established its Bluesky unit to try to work through what a decentralised standard for social networks might look like. There is a risk that whether by accident or by design those types of models engineer away the ability to comply with legislation and at that point that leaves Ofcom with limited measures as to what it does in situations like that. Does that effectively take us to a point where Ofcom has the service blocking powers or nothing? Clearly those service blocking powers for a site like Twitter would raise very significant issues of freedom of expression, if that is the only thing that is left in the tank.

Q101 **Simon Jupp:** Thank you for explaining that in a clear, concise and not at all baffling way. I appreciate that, given how technical this question was.

Susie Hargreaves: I agree with Andy on this. One of the issues we need to be careful about is not being too prescriptive, because technology changes and we do not know what the technology will be like in five years' time. What we must do is ensure there are principles in there and that people need to use evolving technology to fight the problem and to evidence that they are. We also totally agree about the issue of technology notices, which we covered in our submission. Again, how do you assess the prevalence of a problem if you do not know what their problems are on the platform? A technology notice could not apply in relation to encrypted channels.

There is a real problem of perverse consequences where we had the accredited technology issue caused by the European Union with the temporary derogation from the privacy directive, which resulted in Facebook stopping scanning 400 million accounts. We just need to be really careful about the technology notices. We need to ensure that this is principles-based so that we can evolve. Every company has slightly different technology and hashing is a great example where Microsoft have PhotoDNA, Google have their own hashing technology and we just need

to ensure that as something new comes online that we have the ability to respond to that in a technological way.

Q102 **Simon Jupp:** That is going to be exceptionally hard to draft in the next couple of weeks, some principles that cover a multitude of issues that you have raised. That is almost impossible, surely?

Susie Hargreaves: We already have the draft code of practice and we already have when it comes to the illegal content some principles base and we were very involved in the drawing up of the code. One of the things that we are recommending, one of our roles we think we should play in the future, is to help update that code, so we ensure that it is up to date and relevant in relation to what is technologically possible.

If it is principles-based that is possible, but the trouble is if we get into too much detail we are going to be in trouble on the technology front.

Simon Jupp: Interesting.

Q103 **Damian Green:** Briefly, if regulation is going to be effective it relies on trust in the organisations that will inevitably be developing new technology. I am struck by some of the discussion this morning where we are talking about the balance that needs to be struck. In terms of child abuse images, I genuinely do not see what balance you strike. Surely you devote all your energy as a company not to facilitate the spreading of child abuse images. Is that not the underlying attitude of particularly, Susie, your members?

Susie Hargreaves: I agree with you totally, but for instance when we come to look at how does a company address that, in the Bill they have to deploy ways to disrupt the child sexual abuse, or ensure that it is not loaded on to their platforms. They might have their own technology to fight that, or they may use some of ours or have other ways to do that. What we must ensure is that they evidence they are able to do that, and that is why we think there is a role for us to play. We can say to company A or whatever, "Okay, you are not using this blocking list, or this hash list. What are you doing internally?" Some of that is commercially sensitive, but if they were able to provide evidence through a trusted force and obviously Ofcom have the powers to enforce that, that is important.

Q104 **Damian Green:** That is true, but my underlying point I am trying to grasp is whether they want to. Are they doing this because they are worried about the PR, or because there is a regulation that says they must do it, or do they want to do this? What I find slightly odd is that we even must ask that question. I cannot believe that anyone at the top of Facebook wants people to think, "Well, maybe in an ideal world they would allow all this kind of content because they can make money out of it." Please tell me that is not the case.

Susie Hargreaves: In relation to images and videos, it is very easy to negate the things that companies currently do. The current narrative is

that they do nothing, and that is just not true. Companies do currently deploy mechanisms to take this content off their platforms. I am talking about the imagery and the videos, not the grooming and the text or whatever, and the harmful content. Let us just take Facebook. They detect the majority of child sexual abuse themselves, through their own mechanisms. They self-report that, because they have mandatory reporting, which is also another recommendation within this Bill. They report that into NCMEC so that is not stuff that we have forced them to find. They find it themselves and they report it into NCMEC.

When you talk to all the companies, and my experience of 10 years working with the companies, is that they do not want child sexual abuse on their platforms and they do try to find ways to get it off their platforms, but they cannot control people posting it on to their platforms so they need to have a way to deal with that.

That is not to defend them and say that they cannot do more, but I have not met a single person in a company who said, "Do you know what? I am quite happy to have child sexual abuse images and videos on my platform." We need to make sure that we have balance in this and recognise that there is some good stuff that currently happens. We are leading the world in terms of the way in which we work with the industry, but there clearly is so much more that can be done.

Q105 **Damian Green:** That last point you make about the people who post it, or look for it, it is interesting the discussion about anonymity of individuals is often made in the context of abuse of politicians or whatever, but it seems to me in this instance if people could not be anonymous maybe only to the companies themselves that would act as a deterrent for people to go searching for this type of imagery. Would you agree with that?

Susie Hargreaves: I totally agree that if you are one of these bad actors who is consistently searching and these companies do have a lot of information about the individuals as we heard yesterday, then that is where the focus should be. There are reasons why anonymity might be a good thing for some children in terms of safeguarding, so we need to think it through very carefully, but the focus needs to be on the known bad actors and ensuring that they cannot operate in an anonymous way.

Q106 **Damian Green:** Do you agree with that, Andy?

Andy Burrows: Anonymity has benefits for children, but it also clearly presents risks. I think our preferred approach would be that there are clear requirements in the legislation to mitigate the risks posed by anonymity. That could, for example, be giving users the option to verify and then in turn giving users the ability to have greater control over what content they see. Could you then decide that as a Member of Parliament with the degree of abuse that you are receiving that you could filter out comments from accounts that are not verified?

On a related point, there is the right or otherwise to anonymity, but there is also the way in which anonymity in terms of propagating illegal harm can be furthered through a design choice like end-to-end encryption. We know that WhatsApp, for example, have said publicly, I think to the Home Affairs Select Committee, that they remove hundreds of thousands of accounts per month for child sexual abuse material, but that translates into a very small percentage of those accounts going to the National Center for Missing and Exploited Children in the form of actionable intelligence, because there is not the qualifying data to then make a report that can then be passed on to law enforcement.

There are issues around anonymity but about wider design choices and how they can enable abusers and frustrate the ability of platforms to report and detect content and then that to translate to a knock on the door by the police.

Q107 **Chair:** To follow up on that, are you suggesting that WhatsApp are sitting on instances of child sexual exploitation?

Andy Burrows: WhatsApp have been very quick to proclaim that they have identified a third way here. They have found what they consider to be a reasonable balance between privacy and children's safety. I do not accept that is the case. If the vast majority of accounts that they are suspending are not then translating into meaningful reports because they do not have the ability to do that, then those accounts will just continue to pop up. We are not identifying.

Q108 **Chair:** So they are not passing the details on to the police of known sex offenders using WhatsApp?

Andy Burrows: Because they do not have the technical ability to do so.

Q109 **Chair:** You said that they had the technical ability to find this activity going on, so therefore surely they could present that to law enforcement?

Andy Burrows: My understanding is that where WhatsApp are able to act is on the non-encrypted signal, so that is the name of a group chat, that is the picture of the group. Luckily in that respect—

Q110 **Chair:** The front end, not the conversation? Of course, because the others use encrypted, as we know. Surely that is an instance in which if you find something that says something nefarious and vile and has an image that is vile and is a clear potential criminal act, it is beholden on them as citizens, as normal representatives in our society, to contact the police and say, "This group, these are the people involved. Why do you not go and knock on their door?"

Andy Burrows: We simply do not have the transparency about the process through which WhatsApp is then able to arrive at whether that is an actionable report though. I would love to see that transparency. It is a legal requirement under US law for US-based platforms to report instances of child abuse. I think this is then about can they build data

that is sufficiently useful that then can feed its way through the system to law enforcement? That is where the barrier is.

Q111 **Chair:** Is there any mileage in terms of the sex offenders' register, in terms of whether or not potentially this information should be shared with social media platforms and those who are on the sex offenders' register should not be partaking in social media?

Andy Burrows: There are clearly a range of issues there and there is the balance between participation and safety. Where some companies already say that their users should not be able to use their services, so I think that is a requirement that Facebook puts down, what there then is not is a mechanism to share that data. If those platforms that are choosing to take that approach, is there a mechanism—

Q112 **Chair:** In teaching, for example, there is List 99, I believe, which indicates those who have previously been involved in wrongdoing with children in the education sector. List 99 basically means that you do not work again with children. Is there any mileage in terms of perhaps something that is around those who are convicted of offences against children and whether or not a social media company should at least be able to have a duty of care in order to ensure that those individuals are not readily active in terms of being in touch with children?

Andy Burrows: I think if a platform chooses to allow offenders on to their platform then there is certainly a case for increased moderation to make sure that there is not contact with children. This is an area where I think we do need to understand further research, because there have been suggestions that then those with a sexual interest in children can find forms of support through online networks. To be honest we need to understand much more.

Chair: That is a very fair point. There is a whole can of worms in terms of liberty and understanding that, but it is an interesting area to explore.

Q113 **Jane Stevenson:** Thank you to our witnesses. I am going to go back to the use of technology notices that Ofcom are going to be able to issue. You have already raised the Catch-22 of proving that that content is prevalent. What are your thoughts on how this perhaps could be changed especially with encrypted services, but also how global companies are going to make this work in the UK? The other thing, Susie, that you have touched on was Facebook stopped scanning because of an EU regulation about privacy and how this all fits together. Where do you see these notices being improved?

Andy Burrows: If I pick up on this, I think it is a very difficult to resolve Catch-22 and I think a better, more proactive approach would be for platforms to risk assess and for Ofcom to have the opportunity to intervene at an earlier point. So, can a platform through a risk assessment demonstrate that it has identified risks and has taken proportionate measures to address reasonably foreseeable harms? That is consistent with the underpinning of the regime overall, and I think that is

a better approach than technology warning notices in respect of end-to-end encryption certainly.

Q114 **Jane Stevenson:** Do you think Ofcom would need the power to mandate de-encryption, or do you think that is a step too far?

Andy Burrows: This is not an issue of encryption or not. It is an issue of encryption but with mitigation in place. It is an issue of encryption on a service. Encryption on a siloed separate messaging app may be different from, say, end-to-end encryption on Facebook, where this is not just about the encryption of messaging services, but it is the way in which that interplays with, for example, friend suggestions. To take the type of grooming pathway that you would see on a social network such as Facebook, Snapchat or Instagram, an abuser is able to exploit the friend suggestions, the algorithmic recommendations of children, to then—similar to phishing emails—contact large numbers of children, a small number apply and then the grooming process starts in the DM process, but then can escalate into video chats and into the rooms function, which allows up to 50 users who I think I am right in saying do not necessarily need to have an account on the platform to be able to join a call. The fact that all those functionalities are under an end-to-end encrypted cloak, where the platform cannot see what is going on, means that risk profile is markedly higher.

We need to see a risk assessment and this is about understanding the interplay with other design features, how that can be mitigated and can that be mitigated effectively.

Susie Hargreaves: In relation to the technology notices, one of the issues that we could potentially get bound up in is people disputing the accuracy of existing technology. For instance, PhotoDNA is a good example of that, where we have some people who are speaking out in terms of its accuracy. It is the industry standard and the last thing we want to do is to get bound up in court or find that we are in ridiculous discussions about accuracy of standardised technology that will then mean that children are not protected. We are concerned about that.

In terms of the end-to-end encryption, our line on this is not that we will demonise the technology. We use technology and we think encryption is a good thing but there just need to be protections put in place. What we need to ensure is that where certain technologies are being used, that there is equivalency in place and that child protection, child safety, is the overriding factor because children have human rights and rights to privacy as well.

We do not accept the argument that there is no way to ensure that there is safety on encrypted channels in relation to known child sexual abuse images. We want to ensure that the child safety argument is not overshadowed by the privacy argument here. Encryption is a good thing generally but we need to make sure that we have child protection measures in place.

Andy Burrows: Fundamentally if I can quickly come back in, we have seen platforms embrace human rights principles as an approach to content moderation and that is welcome, but all too often that curiously overlooks the fact that in the UK one in five internet users are children and young people, and that is one in three globally. When we start to then see how we balance the range of fundamental rights that are at stake and who they are borne by, and recognition that one in five internet users are inherently vulnerable by dint of being children, we do not see those trade-offs being stacked up. Too often we see right now children being ignored or overlooked in terms of discussions on internet governance and product design, so you will see a situation where Facebook for example is pursuing end-to-end encryption and wrapping themselves up in a human rights framework-based approach, but ignoring the significant part of the user base who are children, because those rights then come secondary to those privileged rights around privacy. We need to get the balance right, rather than privileging one over the other.

Susie Hargreaves: A final add to that, the technology is why working with co-designators and experts is absolutely essential. We will often be working with individual companies on bespoke products and services that they use to keep their platforms safe. We must ensure that we do not get into a situation where Ofcom without that expertise are issuing notices, but working with the experts and the companies to ensure that what we are doing is right. They are held to account; our opposition to this is not that they are not held to account. It is simply that we need to ensure that we do not put something in that has perverse consequences.

Q115 **Jane Stevenson:** Do you think that the balance on part of the notice is that there must be either accredited technology and a mix of human moderators and a complaints procedure? Do you think there is too much reliance on accredited technology and not enough people to get down and examine the content?

Susie Hargreaves: We depend on human moderation so everything that IWF acts on is moderated by human beings, by two people. We have quality assured lists of data that we use, which have had human moderation. At the moment there does need to be a balance because we are not there yet in terms of we just cannot rely on the technology. We need to have that balance and particularly for the IWF I should say knowing exactly what is happening within this Bill is incredibly important, because I have people looking at child sexual abuse every day. It is important that we recognise the importance of the moderator in this and at the same time the importance of the technology. The technology will get better. We just need to make sure that we are constantly innovating and working the two together.

Q116 **Jane Stevenson:** On the complaints procedure element, do you feel that the complaints procedures on platforms are generally robust or quick enough to get down content or deal with complaints?

Andy Burrows: We know from our data and from Ofcom data that children understandably have had a negative experience of reporting content because all too often it is not taken down and there is not sufficient transparency about how or why a decision has been taken. Children, I think probably like all of us in this room, will recognise if you have a bad experience is it worth plodding along trying to repeat that? It is vital that we can get to a point through this regime where children can have greater confidence to report content and also to exercise their legal rights.

Under the Children's Code children have a clear, legal right to remove content. That is very difficult for a child to be able to exercise, because of all the practical barriers, the ways in which that reporting is made hard. We have seen through some of the Frances Haugen reporting in respect of hate speech that Facebook sought to make the reporting process more complicated, to drive down the volume of user reports. That then had the knock-on effect of increasing the share of content that was taken down through AI. The reporting process should be simple and it has to drive confidence.

Q117 **Jane Stevenson:** Do you think it should be different for children? Do you think they should have an easier method of reporting?

Andy Burrows: Absolutely, and there is benefit in considering on the back end how children's reports are processed. Are they triaged effectively? That takes us back to the issue of transparency, which is where there is just opacity about how industry processes work. Are they handling concerns from children in different ways? What is the level of expertise and resource aside from child sexual abuse material where there is clearly a dedicated resource in place? Is there an understanding of child safety issues? Is there an understanding of some of the contextual drivers? The point was made earlier about linguistic, cultural and contextual issues. The answer is we simply do not know.

Susie Hargreaves: Not from the children's perspective, but from the illegal content perspective, we receive reports from the public of suspected child sexual abuse and certainly once a company is notified that they are hosting illegal content they remove it. In the UK we have a world record in the sense that we get content typically removed in under two hours. Once a company is notified that they are hosting illegal content under the e-commerce directive they are criminally liable for that, so they are obliged to remove it. Obviously we do not have those powers in other countries, so that is why we have a blocking list that goes out across the world with content that we have found, which we know is illegal, and it stays on that list until such time as that company removes it.

The removal of illegal content is very quick from our point of view, particularly in the UK. Unfortunately some other countries are not the same, but that is different to the ability of children to report.

Chair: That concludes our first panel. Andy Burrows and Susie Hargreaves, thank you very much for your evidence today. It has been very interesting. We are going to take a short adjournment, about two minutes, while we set up our second panel. Thank you.

Examination of witnesses

Witnesses: Seyi Akiwowo, Rt Hon Maria Miller MP, Marianna Spring and Cordelia Tucker O'Sullivan.

Q118 **Chair:** This is the Digital, Culture, Media and Sport Select Committee and this is our subcommittee inquiring into Online Harms. We are joined in our second panel today by Seyi Akiwowo, the founder and director of Glitch; the Right Honourable Maria Miller MP, former Culture Secretary; Cordelia Tucker O'Sullivan, Senior Policy and Public Affairs Manager at Refuge; and Marianna Spring, the specialist disinformation and social media reporter at the BBC, who many I am sure on this panel will be quite familiar with, having been interviewed a few times.

Seyi, Maria, Cordelia and Marianna, thank you very much for joining us this afternoon for this important session.

Seyi, I think the first question comes to you. Is it possible to effectively legislate against anonymity online?

Seyi Akiwowo: I think anonymity is a tool that is important where you have people able to express themselves online. I think after Gamergate, which negatively impacted lots of women and minoritised communities, we saw the need for pseudo names, we saw the need for ways to be able to protect yourselves online. Anonymity in itself is a tool for fear of expression, but we are seeing small numbers of people use it to abuse and escape accountability. There must be ways that general users of platforms can opt in to interact with other people who have verified their account. I am very lucky to have a blue tick on Twitter and if I, like probably after speaking today, face some abuse I can then choose to opt in to speak to other people who have verified their accounts, whether they have verified their e-mail address, their phone numbers or have a blue tick. That allows me some degree of understanding that people are who they are online and I think there should be better tools to give women—women MPs particularly, women in public life—that ability to decide who they want to interact with.

I also think that legislating around anonymity can sometimes be a mask for some of the real issues around online abuse, which stem from offline. We know that online violence is a continuum of offline violence. If by banning anonymity that suppresses the issue, we need to look at offline education around why people are using these tools, these platforms, to speak the way they speak and behave the way they are behaving.

Q119 **Chair:** Cordelia, do you have any insight into that in terms of the idea that this reflects societal harm?

Cordelia Tucker O'Sullivan: I absolutely agree with what Seyi said. This very much is a continuum. There is no real difference between online and offline in so far as there ever was. We certainly see even where cases where the perpetrator of this online abuse is known and they are identified, so we particularly work with survivors of domestic abuse, so you are talking about a specific perpetrator targeting a specific individual or individual and their children, even in those cases very little action is taken against the perpetrator. We support virtually no survivors where the perpetrator is banned from the platform, certainly very little cross-platform collaboration, even where the parent company owns multiple other platforms. For us our area is less so the abuse of public figures, but we agree there ought to be nuance when considering the issue of online anonymity. Fundamentally even where they are known it is still quite obviously to us not enough for platforms to then be able to take action.

Q120 **Chair:** Is there a caste system in place when it comes to online in terms of blue tick or no blue tick for example on Twitter and how seriously things are taken? You have just outlined there clearly traceable individuals who are taking their offline aggression and mirroring that online, yet no action is taken. Yet someone can be abusive to someone else, a footballer and so on, make a horrible remark and it is quite right that that is certainly examined and looked at, yet they have a knock at the door by the police. Do we have that side of things wrong or is it just a matter of the police being too busy as well?

Cordelia Tucker O'Sullivan: First, when it comes to the police response to offline domestic abuse and violence against women and girls, it still lacks that sense of priority that it ought to have. We saw from a recent HMIC report into the police engagement with violence against women and girls that one of the core messages is that it needs to be at the same priority as terrorism. In this Bill, which explicitly refers to child sexual exploitation and abuse and terrorism and nothing about online VAWG, I think we see that there is a lack of prioritisation in both offline and online, but here we have a piece of legislation that is definitely reinforcing that. That is why we think it is so important that online violence against women and girls is explicitly included, otherwise the effect is to deprioritise it yet again and to replicate what is existing already in this space.

Seyi Akiwowo: I think there does need to be wider education and consistency among police forces. We deliver workshops for women in public life, but also the general public, on how to stay safe online. Time and again we are met with, "What is the point? We report it to the police and it does not get listened to. We get told to just come offline" and that continual victim-blaming and gaslighting is causing further trauma to women who are facing some horrific behaviours online. I definitely think that legislation that includes women in the Bill through duty of care, through harm, through legal but harmful, throughout the entire Bill, is

key so that police teams are held to a standard to ensure that they are enforcing the law and keeping women safe online and offline.

Mrs Maria Miller: The Bill is silent on one of the issues that is most pressing for our constituents, the problem of abuse from anonymous accounts. In fact, I just saw something on my own Twitter account saying, "There is an obsession with anonymity." Well, it is an obsession because that is where a great deal of abuse comes from. The research that has been done by Glitch and the Violence Against Women Coalition shows that 84% of people experienced online abuse from strangers and so often accounts that they did not know before the incidents occurred.

What I would like to see this Bill do is to take up the idea of verified accounts by default. At the moment the default is anonymity. It should be that people default into having a verified account. We know that four in five people will be wiling to upload some form of ID to gain a verified account and that three in four would support action to tackle anonymous accounts. This is something that is missing in the Bill. I hope this Committee calls on the Government to deal with it, because it is something that our constituents want to see tackled.

Q121 **Julie Elliott:** Maria, do you think the debate about freedom of expression regarding the Bill and the duties to protect freedom of expression within it, accurately reflect the experience of women and girls online?

Mrs Maria Miller: No and that is for a number of reasons. First, the Bill does nothing to tackle some of the shortfalls in the law at the moment. That means that we have a potential situation where the duty of care will come into play against a context of legal framework that has holes in it. The idea of trying to say that posting nude or sexually-explicit images online, because it is not unlawful, is part of freedom of expression I think is a debate we would see happen if this Bill did not tackle some of the shortfalls in the criminal law. That is the first point I make.

The second issue we will need to think about if we do not tackle the shortfalls in the law is the issue of legal but harmful. That is very much at the heart of the freedom of expression debate. It will also become muddied because at the moment it is entirely legal to post images of male genitalia online, which in the offline world would be seen as indecent exposure but in the online world will be seen as legal but harmful. That cannot be right.

Therefore my argument will be, and there are probably many others with me, that by not addressing the holes in the law you will end up with a very warped discussion on freedom of expression.

Cordelia Tucker O'Sullivan: I would like to come in. Obviously the Bill has been criticised for its implications for freedom of expression. What irks me, and I am sure is shared by some of you and other panellists, is that it essentially ignores the free expression of women and girls when we are having this debate. There is this false dichotomy of the rights of

women and girls versus free expression, which forgets that women are humans with human rights as well. They are effectively being prevented by accessing what is the modern town hall of the day, even more so in the pandemic. This is where the substantive debates on the news of the day are happening, not to mention remaining connected with friends. We know from the survivors we support that isolation from friends and families is one of the most common tools perpetrators use as their pattern of coercive and controlling behaviour.

To give a flavour of the sorts of issues we are seeing, a survivor we worked with said her ex would, "post horrible things, threatening things like, 'tell Deandra I'm coming for her', sending me loads of private messages. He hacked every single social media account I had and then changed my passwords. He would contact me through my professional and personal accounts with messages, hundreds of messages. If my employer posts anything on social media he will comment on there." I do not think any of us would argue that this survivor's freedom of expression has not been significantly hampered by the fact that these platforms are not safe and by the fact that platforms are not responding in a way that keeps users, particularly women and girls, safe.

Q122 **Alex Davies-Jones:** Thank you, Chair. Before I ask my questions I should probably declare an interest as the Chair of the all-party parliamentary group on perpetrators of domestic abuse. I work quite closely with Refuge and Maria and the group.

Seyi, if I come to you first, what has been the response from the tech companies, from these platforms, to the prevalence of online abuse, specifically referring to violence against women and girls and particularly during the pandemic?

Seyi Akiwowo: To be respectful, the response from tech companies has not been great. I think Frances's testimony yesterday in Parliament shows that they knew more than they were letting on. There has been a series of giving civil society groups the run around to provide evidence of women's experiences online.

We knew that online abuse was already an issue for women before the pandemic. Globally, women are 27 times more likely to be harassed. It is really important to talk about intersectionality here because we know that it is worse for women of colour, worse for women with disabilities, worse for women from LGBTQI+ communities. This was already a problem before the pandemic. In lockdown last year we saw there was no effort from tech companies to address this. There was lots of investment in looking at Covid disinformation yet gender disinformation went through the roof and there was no response. We saw that online abuse had increased during the pandemic and we have not yet seen tech companies have transparency around their policies, content moderation and safety tools so women can at least try to mitigate some of the harms.

What is also really frustrating is that we see tech companies working very closely together when it comes to child exploitation and terrorism, which is fantastic. However, when it comes to women and violence against women they are absolutely silent. There is no cross-party collaboration among the companies. That is where it does feel like profits over people. We work with survivors who tell you that a troll does not just stop on YouTube or on Facebook. If they want to find you they will find you on every single platform. Therefore when one tech company is not talking to another, you are only making it harder for women and people to get access to justice.

Q123 **Alex Davies-Jones:** On that point, where a troll or an abuser will follow you from platform to platform, is there evidence this also escalates into offline actual physical abuse, abuse in the real world rather than just online?

Marianna Spring: A "Panorama" investigation I did recently on this topic looked at that. The UN commissioned some research that specifically went into the offline harm that is associated with online harm. One in five of the respondents to their survey spoke about stalking, harassment and all kinds of offline harm that is associated with the online harm.

It is something I worry about. Doing my job I experience a lot of online hate. Almost every woman I interviewed raised it as a concern, they fear the offline harm—not just psychologically on them and the impact it has in making them feel like they do not want to use social media anymore—but actually that they feel frightened and worried when they are going to work or going about their jobs. As has been highlighted by everyone here, for many of these women—whether politicians or influencers and not just people in the public eye, I hear from librarians, firefighters and doctors—who use social media as an extension of their job, it is essential to be a part of public life and a part of that conversation. Online hate is having a detrimental effect and making it very difficult for them to do their jobs.

Cordelia Tucker O'Sullivan: To come in on this, in response to this growing threat of tech abuse—which is what we call it—and intimate partner abuse conducted online, social media platform abuse is the second most commonly reported issue just behind security issues with devices to our tech abuse team. Their caseload over the pandemic—there was some talk about that—has more than doubled. This is a growing issue, which is why we set up the tech abuse team a few years ago. It is absolutely getting exponentially worse.

We know there is a very strong relationship between online abuse and offline harms. One of the recommendations we are making for the Bill is that domestic homicide reviews are empowered to make recommendations to platforms because we know they feature in a huge amount of cases. Almost every single phone call we get to the National Domestic Abuse Helpline that we run has some element of tech abuse,

which is wider than social media but a very large proportion of it is based on social media.

As Maria referenced, this sort of two-tier approach, both to how we regulate interactions and the criminal law as well, does not make any sense because we know this type of distinction between online and offline is not real, certainly for the survivors we support

Mrs Maria Miller: Alex, the Government's strategy is that what is illegal offline is illegal online. That is their strategy and has been since I was Secretary of State, which is many years ago now. However, we still have significant gaps in our legislation to make that a reality. Cyber-flashing is one, deep fake is another and intimate image abuse is another. If we are not careful, what is a golden opportunity—the Online Safety Bill—could be a missed opportunity if we do not address those holes in the law.

The duty that is going to be put in place by this Bill, the duty on social media providers, is absolutely directly dependent on the criminal law and the broader laws. If we do not get those right then the duty will be diluted. Therefore it is important these things go hand in hand. If they do not, the Bill will do little for people who want personal redress. It will be about regulating social media companies without enhancing and improving the ability for the individual to get redress when harm is aimed at them directly.

Q124 **Alex Davies-Jones:** Why do you think it is then that online abuse and violence against women and girls has not explicitly been placed on the face of this Bill as a provision?

Mrs Maria Miller: I think it is, very candidly, because the Bill is trying to be very discrete, as in very focused, in what it does for fear of becoming a 'Christmas tree' Bill. All of us in this room probably have different things we want the Bill to address, which is part of what the Government are trying to do in tailoring and focusing it so sharply in on social media regulation. I argue though that in doing that they are producing something that will disappoint many people who need to see the law strengthened. I, again, pitch the fact that intimate image abuse has to be one of the vilest ways you can abuse somebody online. Whether you are a man or a woman, whether you are gay or straight, whether you are married or not, having a nude or sexually-explicit image of yourself put into the general public is horrendous and can devastate people's lives.

I would also draw the attention of the Committee to new software that is specifically designed to 'nudify' images of any of us in this room; actually, no, only the women. Software has been designed to take pictures of the women in this room and make them appear as if they are naked; not men, just women. That is currently totally legal. It cannot be right. If this Bill does not address these issues then it will be missing a major issue that our constituents face.

Seyi Akiwowo: Thank you. It has been great to see different Secretary of States, when talking about the Bill, understanding the importance of violence against women. It has been great that we have seen combined characteristics be mentioned in the Bill. That has been progress. However, we do not want it in announcements. We do not want it in journalists' articles. We want it in the Bill. Whether deliberately or not, violence against women and women's experience of the online space has been missing and that is 50% of the population.

Having an understanding of the gendered way online harms take place supports children. We cannot see children as a homogenous group. We know from Girl Guiding and Childnet surveys recently that girls' experience in the online space is different than boys. Therefore having gendered language is important to make sure we are capturing the women who are disproportionately impacted, especially women of colour. The word "children" is mentioned 213 times in the Bill, "terrorism" is mentioned 55 times. Neither "women" nor "gender" are mentioned at all in the Bill.

If I may, there was an incident in Cheshire where a guy was in court for, for 10 years, stalking hundreds of women. As Maria Miller was talking about, he was taking intimate photos of them, creating fake photos of them and pretending to be them on social platforms trying to get them fired from work. It was hundreds of women over 10 years. The judge, herself, said there has been such a focus—I have to say by everyone—on offline safety that we have not put enough attention on social media to make sure they prioritise women's safety. We cannot claim this Bill to be putting safety first if it does not put 50% of the population at the heart of the Bill.

Q125 **Alex Davies-Jones:** Currently as it stands the Bill, as you said, does not contain the word "women" and does not focus on violence against women and girls. Have you heard from Ofcom about how, if it does, it plans to treat this as a priority going forward and to focus on this issue specifically?

Seyi Akiwowo: Ofcom has been open in working with us at Glitch and other civil society members to get ready for being the regulator. What they have said is that if it is not in the primary legislation it will not be a priority. They are asking us to ask you to make sure this is in the Bill. We cannot leave it to chance. We have waited five years for this Bill. We cannot wait another five years for a secondary Bill when every day women are being abused online.

It is also important to say that when we talk about terrorism we also need to talk about the growth of 'incels', the growth of groups that are deliberately recruiting and radicalising men and boys in our country to hate women. There is an element of gender-based violence that is impacting terrorism as well. Therefore if we only focus on terrorism we have not done a good enough job there as well. By making sure we are

prioritising women's safety we can make sure we are reinforcing children's safety as well as terrorism.

Cordelia Tucker O'Sullivan: It is quite odd that in the tackling of VAWG strategy the Online Safety Bill is mentioned only with regards to children, which is very strange. It almost makes you wonder if they are asking for us to push them on this.

As Seyi said, we have heard so much rhetoric about the importance of prioritising violence against women and girls but not that much prioritisation going on in concrete ways that go beyond the criminal justice system, which is slow. The criminal justice process takes a long time. The point with this regulation is that we are asking for platforms to take responsibility, to build in safety by design, to build in appropriate reporting mechanisms that, for example, do not require women to report every single individual piece of content that, beyond being incredibly burdensome, is extremely traumatic.

I think all of us on this panel have likely been subject to these sorts of threats. Thankfully, in my own experience, I have not had to look at a single one of them because that is something we have a team to do. That being said, they certainly have to experience it. What we have seen, from the HMIC report into engaging with women and girls, is this call to arms from many who we do not normally hear use that sort of language to prioritise violence against women and girls. We do think this is a big opportunity to do that. We can embed this throughout the Bill, throughout the surrounding policies. As Seyi said, Ofcom is a regulator with a big job. If we do not make sure this is a priority when there are two other categories of harms explicitly prioritised it is not going to be able to do it. Therefore they need it to both be specifically legislated for and prioritised, as well as given the resource to make sure they do their job well and we make some headway on this issue.

Q126 **Clive Efford:** Thank you, Chair. Just briefly, the HMIC report recommends a multiagency approach to changing attitudes of men, in particular, to deal with this growing issue of violence against women and girls. We heard the evidence of Frances Haugen about Instagram yesterday and what is taking place on there. We had the Ofsted report back in June that highlighted young boys sending unsolicited material to young women and how many young women reported that, which was nine out of 10 in that report. It was a shocking figure.

You learn these attitudes and online is one of those places where clearly those attitudes are instilled. Does this Bill do enough to address that?

Marianna Spring: One thing that is possibly relevant to this is that during the "Panorama" investigation we wanted to see what the kinds of accounts that are sending out abuse are coming across on their social media feeds, not specifically just younger people but across the board. We set up a dummy troll account based on accounts that send me abuse so it was predominately engaged in anti-vaccine and conspiracy content

but also a small amount of misogyny. It was totally private so it was not sending out abuse to other people but it was trying to test the algorithms. What we found, after just two weeks, was that on Facebook and Instagram in particular this account, "Barry the troll", was being pushed almost entirely to suggested accounts and pages linked to misogyny, very extreme discussion about rape, harassment, sexual violence and some posts linked to the 'incel' community that Seyi has already mentioned. That was almost all of what was being promoted and suggested by the social media sites.

Therefore I think there is an important discussion to be had not only about, as has been mentioned, what the social media sites are doing to remove the hate that exists on their platforms but what they are showing to the users who then can find themselves, in the case of this dummy account, sucked into a world of yet more misogyny and more extreme content. We have seen—for instance, when it comes to conspiracy theories or disinformation—they are capable of deprioritising their algorithms to not promote that kind of content. "Barry the troll", who mainly liked anti-vax stuff when I first logged on, hardly had any anti-vax stuff. I was quite surprised as I have spent 18 months covering the harm that has caused. Instead, he was being pushed to misogyny after misogyny and really explicit stuff.

There is a dual harm to this, not only to the women who are impacted by the abuse that this account might be emboldened to send out or the women who are affected by that content but also the men themselves, the "Barrys", the people running these accounts who are being sucked into these quite extreme ideologies and sent this hateful content. They are also not being protected.

Mrs Maria Miller: Clive, you have raised an important point. No one Bill can address all of these issues. That is why the Violence Against Women and Girls Strategy is so important. The Women and Equalities Select Committee did a series of reports on sexual harassment in schools, the workplace and general public. It found that a whole range of measures was needed. I was grateful to the Government for the fact that following those reports, and the reports of a number of other Select Committees, sex and relationship education was made mandatory for all school-aged children for the first time after a 20-year debate as I am sure you will remember being, like me, a longer-serving Member. This is just the start. If we are teaching children in school about respect, about consent and about the importance of decency in the way we treat each other, this is part of that.

The second thing I will say to you is that the Government already know, because they have the research, there is a link between extreme pornography, which is often viewed online, and domestic abuse. That also needs to be part of their Violence Against Women and Girls Strategy. At the moment that strategy is a bit too thin on some of these issues, I think it needs to be 'beefed up'.

Q127 **Clive Efford:** My point was more specifically about young men, the attitudes they are learning online and the habits they are getting into by using accounts through Instagram, where many of them should not be because they are too young. Is this Bill a place to address that and, if so, does it do enough?

Seyi Akiwowo: I think there is an opportunity for Ofcom to be investing in digital citizenship education. At Glitch we coined the term "digital citizenship education" to mean rights and responsibilities. That is the same way we have rights offline. The right to go to school, we must be responsible when we go to school. When we have the right to vote we must be responsible with voting. We do not yet seem to have set that social standard and social knowledge when it comes to the online space and what we expect of users.

I do think there is a role for Ofcom to be investing in education so it is not just punitive, it is not just enforcement but it is looking at education. If we do not have a public health approach to ending online abuse we are only going to be increasing the pipeline to prison. We are only going to be sending young boys, who have only been learning this behaviour online through no fault of their own, to prison. We need to intervene, to make sure we are helping young boys to not believe or fall into this gender disinformation that is being shared online.

The Wilson Center in the US did a study around the impact of gender disinformation. It was interesting to see it framed, gender stereotypes as disinformation. If we saw the level of input and investment that tech companies placed on Covid misinformation and disinformation in gender disinformation it would be phenomenal.

I call on this Bill to change the power dynamics. Why are you not prioritising women's safety? Why are you not investing in prompts that are helping men learn about society in a better way? Why is it so easy for algorithms to be teaching us? We are often on the end of the spectrum, having to tell companies to do better. Why can we not now say, "Why are you not doing enough?"?

Cordelia Tucker O'Sullivan: To build on that, if I may, I think what we are essentially getting at is whether we can use this Bill to target directly perpetrators or potential perpetrators who are—for example, as Marianna said—being shown all this quite extreme content. The other question is whether the Bill can do the whole thing when it comes to tackling misogyny.

The first thing is that safety of women and holding perpetrators to account are very much two sides of the same coin. When we speak to survivors one of the biggest things or their top priority when it comes to perpetrator consequences is that they are removed from the platform and cannot just set up another account, which is quite obviously fake, targeting the same individual over and over again with hundreds of harassing messages. We have recently supported a survivor who received

messages from over 200 individual accounts across multiple platforms, and very little was done by the platform in order to tackle this.

We know the response from platforms is poor and the Bill can tackle that. There has to be minimum standards when it comes to reporting practices, when it comes to what platforms then have to do. We then have to have transparency about that.

We need to have transparency reports published for online VAWG happening across different platforms. We need that to be disaggregated by race, sex, gender and the other protected characteristics because we know that black and minority women experience this at even higher rates than other women. We need to know exactly how much is happening on platforms and what they are doing about it.

When it comes to this longer justice, the criminal justice response, it also needs to be vastly improved. At the moment there is not very much co-operation between platforms and the police. The burden is almost always put on survivors, "Can you go and take screenshots of that?" They submit it to the police and they are going to lose that file. There is a lot of difficulty when it comes to resourcing of the police for online crime.

While with this Bill we very much think the focus needs to be on platform responsibility, I absolutely agree with Maria that the gap needs to be closed for content that should be illegal but is not because it makes it much easier for platforms to take action. The other part of that is that the police also need to make this a priority. In many instances getting the police to take domestic abuse seriously is very challenging. When you add an online element it is even more so, in our experience.

Q128 **Jane Stevenson:** I am going to go back to the law. Maria, you have already mentioned that cyber-flashing is not an offence. The Law Commission did recently recommend that cyber-flashing, assisting self-harm and sending threatening communications need to be made offences. Do you think these recommendations are being taken seriously enough by DCMS as they work on this Bill?

Mrs Maria Miller: Jane, I think they are being taken very seriously indeed by successive Secretaries of State. The problem is getting them into legislation. The Law Commission has been looking—whether it is cyber-flashing or intimate image abuse, which directly relates to the efficacy of the Online Safety Bill—at these things for three, four or five years. With the best will in the world, this is a Government with a heavy legislative agenda. If we do not take the opportunity to directly address these issues now within the context of the Online Safety Bill, I fear it is going to be difficult to find room to do it at another point in time.

I do think people take this seriously. I think the recommendations that have come forward from the Law Commission, both on cyber-flashing and intimate image abuse, are extremely strong. There are, of course, always changes to be made but I am hoping that the timing of the Online Safety

Bill now will perhaps enable the Government to think again and fill it in, put into this Bill these sorts of strengthened criminal measures so that all of our constituents can see a very, very direct benefit and strengthening of the law that the police can then react to accordingly.

One idea I can remember raising on Second Reading of a Bill similar to this was, "Why are we not looking at levying on social media companies the cost of policing?" You, I am sure, Chair, will have gone to see your local police unit that is monitoring online crimes, particularly around social media, and will know the costs for the police associated with policing this area. Why do we not levy social media companies in the same way we levy football organisations for policing of their matches? It would certainly be a way of trying to get more resource for the police to make what we are discussing today effective in practice.

Q129 **Jane Stevenson:** I would like to open a little broader question on cyber-flashing. There has been some criticism that the offence recommendation is for the motivation of the person sending the pictures, which would either be to cause harm or obtain sexual gratification. Do you think that is the right approach to cyber-flashing and do you think that is the way to improve the experience for women and girls online?

Seyi Akiwowo: No, I do not think we should be focusing on motivation. That is why a lot of the communication Bills or legislation we currently have, which women are trying to use to get some form of access to justice, make it difficult for them to get any form of justice because they are having to do that work to prove that person was malicious in their abuse.

We agree with Professor Clare McGlynn's recommendation to the Law Commission that we should not be looking at motivation, but instead recognising that the threat and the invasion of privacy in itself is enough. An actus reus, if you like; if you have done it, it does not matter about your motivation. You have that with highway offences. It does not matter if you did not mean to speed, it does not matter if you did not mean to run across the red light, it is the fact you have done it and it was causing harm to other road users. That is the analogy we should be using with the online space. It is everybody's responsibility to make sure our roads are safe, everyone is following the rules. We should be having that applied to the online space as all our responsibility.

Cordelia Tucker O'Sullivan: I absolutely agree. To follow on from what Maria said around parliamentary time, we had very similar pushback when it came to Refuge's campaign to criminalise threats to share intimate images, which was made a criminal offence as part of the now Domestic Abuse Act. The timing of the Law Commission review and this Bill is even better so I think it is a good opportunity for the Government. While it is criminal legislation we are talking about, it has a direct impact on the ease with which platforms can take action. I absolutely agree this will be a really good opportunity to do that.

Reflecting on the threat to share campaign, one of the biggest issues is that the intent element is still there and it makes it extremely difficult to prosecute. It is an issue with the existing offence. We think it will be a big mistake to replicate that for a new offence. When talking to various legal professionals they say any lawyer worth their salt is going to argue that they did it for a laugh, they just did it because they were not thinking or any number of reasons for sharing it that do not fall within the intent to cause distress or humiliation.

One of the vital functions that our specialist tech abuse team provides is to support making those arguments, to support the survivor when reporting to the police. However, we are severely underfunded. This is a national service that stretches across the majority of areas in England and yet we receive virtually no funding or sustained funding. We absolutely agree that one of the things the Bill could be used to do is to use a percentage of the fines levied and filter them towards specialist services, like Refuge's tech abuse team, like the Revenge Porn Helpline and a myriad of other organisations that could, for example, take on casework but are underfunded and cannot do so. That is a vital part of supporting and enabling survivors to take action, both for illegal and for harmful content.

Mrs Maria Miller: Could I echo that point? Year in year out it feels like we are going from hand to mouth in terms of financial support for the organisations that are helping victims. This is a complex crime to unpick, to get things taken down and to get the sort of peace of mind people need. We have seen from the Revenge Porn Helpline that cases have grown over the last 12 months by 87%, yet it has struggled to get increases in its funding. I certainly will be considering an amendment to this Bill, to make sure proper financial support for victims' groups is on the face of the Bill because it is such a complex area to tackle yourself.

Q130 **Jane Stevenson:** Is some of the problem that this is moving so quickly, the law is not keeping pace and there are people, I am sure, devising other methods of abuse in their bedrooms as we speak? Do Government have responsibility to be more proactive about keeping pace and making sure it does not fall behind?

Mrs Maria Miller: Can I come in there? I think that is an excellent point. It is very worthy but not the right solution to keep tackling individual forms of abuse. It is slightly straying, Chair, please bear with me. Upskirting is a good example. It is very important that we need to outlaw it. It is dreadful it is not outlawed, particularly when those images go online. However, we are not tackling the broader issue of intimate image abuse. It would be entirely wrong, I think, for the Government to come forward with individual recommendations around cyber-flashing or deep fake. What they could do is a catch-all law, which is what the Law Commission is proposing, which will make the taking, making and sharing of intimate images unlawful, a criminal offence, and, indeed, I think a sex offence as well because these things have a devastating effect on

people's lives. It is a catch-all rather than trying to do 'whack-a-mole' every time the industry changes the way women can be abused.

Seyi Akiwowo: I completely agree. A catch-all legislation will be important. A catch-all form of education and approach is also important. We cannot be teaching this and the next generation how to use specific platforms because they might not exist. I have friends who have kids who would dare not to be on Facebook right now. There is no point trying to have specific legislation or education pieces for particular platforms. What we need is an understanding around behaviours that we expect of people online. We have not set that standard yet. We have not said, "What is our duty of care to each other online?" How are we active bystanders online? When we see someone facing abuse, how are we making sure we are not scrolling past but we are also helping to report it and helping to support them? How do we make sure we are building people up online to be able to hold tech companies to account? We have citizenship classes that teach us how to vote, how to use local councils and how Parliament works. It is fascinating. However, we do not have a course on how tech companies work and how algorithms work so we can now build a new generation of digital citizens who can be holding tech companies to account.

I do think this legislation has an opportunity to copy what has already been done and is working well in Australia. They have an e-safety team that looks specifically at new offences, works specifically on women's harms and is always staying ahead of the curve. There are ways to have arm-length bodies and to fully equip and resource them to make sure they are staying abreast.

If we do not also fundamentally address some of the ideological framing around this—it is something women need to put up with and this is just part of being a woman in public life—this is going to play out in different ways. This is just the fruit of a symptom that we need to start rooting out. That is why we are really, really passionate about a public health approach to ending online abuse, looking at offline violence and online violence and also addressing the trauma of abuse. We have not even talked about that.

We have spoken about access to justice for victims and how difficult that is. However, what happens once you get your court case? Statistically it is small but hopefully you manage to get a win. Then what? You are still having to relive all of that trauma. We know that trauma spreads. We know that violence spreads.

We have learnt how effective a public health approach is for tackling youth violence in Glasgow. I would like to see something similar here for women because I, honestly, am worried for the next 10 years when we start to see the impact of all the women who have been abused now in 2025, 2027 and 2029.

Jane Stevenson: Thank you. Good online citizenship is a very

worthwhile cause.

Cordelia Tucker O'Sullivan: I remember when I was a kid we had Myspace and Bebo and all these different platforms that are defunct. I do not know if they are even working anymore. You have new platforms coming out every five minutes. What all those platforms, existing and new ones, should be required to do is to embed safety by design. What we end up doing—this is what our tech abuse team does—is identifying new features that are, frankly, going to be a disaster for the women we support. We recently had to engage in quite a significant private case—I will not disclose who it was with—where they were releasing new features that our tech abuse team lead described as, "It looks like it was designed by a perpetrator" to make it easy to stalk women, to see their location in real time and she might well not know about it.

These products and features of social media companies are designed without really thinking about it, certainly not in the way we need them to, because they are so unsafe for the women we support. We think it is an opportunity for this Bill, to require that safety by design is embedded throughout the entire product development process.

There are a couple of other upcoming Bills, such as the Product Security Bill when it comes to smart home devices. That is much broader and I will put that aside for now. However, it should be embedded across all these pieces of work. That is a way we can ensure that it does keep pace with new and emerging technologies.

Q131 **Chair:** On that point, Cordelia, does the global trend towards greater encryption rather than less encryption potentially undermine online harms legislation in the UK?

Cordelia Tucker O'Sullivan: It is a difficult question. It is probably beyond the scope of my particular expertise. I was listening to the previous panel when it spoke about the need to balance encryption with safety. When we had the recent proposal, I think from Facebook, to encrypt all of these communications it had an impact on the ability, for platforms and the police alike, to investigate very serious crimes. While, as I said, my expertise is somewhat limited, it is certainly the case that these need to be balanced and we have seen that has not been the case.

Q132 **Chair:** If a company introduced that it is failing in its duty of care, is it not?

Mrs Maria Miller: Chair, I think you are absolutely right. This is why we have to take a step back and look at these broader principles. You are right, encryption could have a great role in undermining the safety of women and girls and, indeed, all of us because of its use by those who wish ill on our society. If we have a duty of care in place for those who are providing these products then you have to ask a deep question as to whether those encryption devices are fulfilling the duty of care that is on the organisation.

The Government are already doing work on safety by design and obviously there have been regulations published already on that. However, how can we make sure that encryption is safe by design? These are the challenges. When I, a number of years ago, went to Silicon Valley and started the discussion on some of these things with the social media companies, the notion that they would be producing products that were safe for society was an anathema. They produced products because they could. What we are doing now is playing catch-up through this Bill, in putting in place the sort of safety that we take for granted in every other area of our lives. I pick up a pen, it will be subject to regulations. I pick up a bottle of water, it will be subject to regulations. However, I pick up my iPad and there is very little governing what is going on in there. That is where this Bill comes into play. It is so important. In many ways we have to be cautious about expecting it to do absolutely everything.

Q133 **Chair:** You made some very specific asks, if you like, of this Bill. This is supposed to be enabling legislation, which is the purpose of it. How do you marry that up if you have very specific acts and yet you want to have an enabling architecture? It is difficult to think of one with the other.

Mrs Maria Miller: Chair, you are absolutely right. I suppose if I had a perfect world I would have two or three pieces of legislation going through this place at one time. We never do that, we do not have suites of legislation that complement each other. In an ideal world I would say to the Government to have another Bill that puts in place some of these criminal sanctions that I have been talking about. It is not going to work as a piece of legislation in the way in which our constituents need and want it to work unless those criminal sanctions are also put on the statute book, particularly with regards to intimate image abuse. I feel very strongly about some of the issues to do with children as well. However, with intimate image abuse there are so many areas there that are, frankly, not against the law online. Somebody can send me a picture of their genitalia online. It is flashing. It is indecent exposure. That is a sex offence if you do it in person, and as an individual, let alone as a woman, that does not feel like a different act by the individual, but it is treated completely differently in law. I fear that the Online Safety Bill will not have the effect and the impact that even the Government want it to have, unless they clean up the criminal law as well.

Q134 **Chair:** I am really tempted to ask you what you would rather, whether you would choose a broader scope for the enabling aspect of this legislation, effectively to introduce duty of care for women and girls, or whether you would rather have the more specific legislation in place.

Mrs Maria Miller: Chair, my experience in this place tends me towards the specific. The law works much better when it comes to specificity. If you have a problem you want fixed, have a law to fix it. While I absolutely respect the need for having duties of care in place, that does not give me the fix for the woman who gets in contact with me because nude and explicit images of her have been sent to her entire family, or they have been posted on a Facebook page, or they have been

distributed through other forms of social media. Duty of care will work in the longer term, but for the short term we need to fix the criminal law as well.

Q135 **Chair:** Marianna, you have experience with this internationally as well. I know that, having read a lot of your stuff. Are similar debates going on internationally, to this degree, when it comes to the duty of care and the need to legislate in order to protect the experience of women and girls online?

Marianna Spring: There is a huge conversation going on. In fact, a lot of the UN-commissioned research that was part of the "Panorama" investigation looked at the experiences of women all over the world. We find is that experience can vary according to where you are. There are some countries, for example Mexico, where there are higher instances of femicide and violence offline. You see that also in some Arab countries. You see how that links with the online violence. What struck me during the course of the "Panorama" investigation, and also from speaking to the UN and the different women they had been interviewing, was the universality of this experience. Women here in the UK, or in the States, or who live in Tunisia, or live in Mexico are all receiving very similar messages online that are calling for them to be raped and are calling for them to be executed. It does not really matter what they do. They can be politicians. They can be journalists. They can be doctors, nurses, or various other people. If they experience racism, homophobia or other forms of discrimination that abuse is even worse.

It is really striking that it is so universal, and it is having such an impact on these women, including here in the UK. They speak about everything, from their fears about it deterring them from certain careers or public life, to their fears of physical harm. Yet, it feels to them as though the conversation has not moved on, that the onus is on them to protect themselves, that the social media sites are not protecting them, that law enforcement is not protecting them, and that no one is listening to them. During the course of our investigation the dummy troll experiment revealed the role that Facebook and Instagram, in this case, played in promoting hate, which is something they say they do not do. They told us they try not to promote hateful content and that they prioritise the community's safety over money. That shows partly the role that they are playing.

Also, law enforcement, the police; the Met said they take online abuse really seriously. That has not been my experience with the police. I feel as though rape and death threats I have had, including from someone who appears to have a prior conviction for stalking and harassing a female police officer, have not been taken seriously at all. Absolutely nothing has happened; no progress. My experience, which was at the heart of the "Panorama" investigation, is so universal, and I do not get racist abuse, or homophobic abuse, or any of the other awful stuff that

people experience online. It is important to think about it in a global context, that women everywhere are experiencing this.

In the UK, we are probably having one of the most positive and productive conversations about how we can protect those women, which a lot of the rest of the world is looking at. That is important.

Chair: We just have to get it into the Bill now. That is the thing.

Q136 **Simon Jupp:** I have more questions for you, Marianna, if I may. On the side, I did not follow you previously on Twitter. I now do. It also comes up with suggested follows. On those suggested follows were an anti-vaxxer, the majority are anonymous, mostly men, and a butcher's shop. I think it is rather odd when we look at this, and I look at the list of people who have been suggested to me that includes an anti-vaxxer and includes the very people that you have been working so hard to point out the issues they raise. On the programme you did, "Online Abuse: Why Do You Hate Me?" you touched on the fact earlier on that as a result of that you and your troll Barry came across an awful lot of misogynistic abuse. Why do you think that was? It could also connect to what I have just said about your Twitter account.

Marianna Spring: It is important to understand, first, how we set that account up. That account was based on accounts that sent me abuse. Like I said, it was really engaged in anti-vaccine and conspiracy content, and it predominantly had liked pages, or followed accounts, or watched videos related to that kind of content. Because Barry had five different social media accounts we would engage in slightly different ways on the different platforms according to how it would be best to test those algorithms, and we did so, obviously, under the editorial policy guidance of the BBC, and from Chloe Colliver, who is an expert at the Institute for Strategic Dialogue. Because we wanted the social media sites, we wanted the algorithms, to know this was a troll, to know this was an abusive account, we also had to engage in some misogynistic content. The account did like a few pages, did post on its own private wall, not to other users, so there would be some indication that this was an abusive account.

Ultimately, we were trying to test whether trolls are promoting more hate, and specifically whether misogynistic trolls are promoting more misogynistic hate. As soon as we logged back on, particularly on Facebook and Instagram—less so on YouTube and far less so on Twitter, and on TikTok a lot of the incel content and extreme misogyny was banned—we were almost immediately proposed other accounts related to this. This is the issue. It comes as no surprise to anyone that if you like dogs, or you want to buy a pair of jeans, you get loads more adverts to buy jeans or you get loads more pages about dogs. The problem is that the social media sites have repeatedly committed to removing hateful content on their platforms. They say that they do not allow hate. So why are they suggesting and promoting hate, hate that is specifically targeting women, in this case, to users?

As I said, with conspiracy content and disinformation I have spent a lot of time covering the real-world harm they have had. Finally, now we are seeing how they are able to deprioritise, not promote, and remove that kind of content. Why is misogynistic hate not taken seriously in this way? Particularly as someone who experiences it personally, it shocks me that that it is happening. Chloe Colliver, who advised us, pointed to what we talk about a lot, what Frances Haugen spoke about yesterday as well, the business models of these social media sites are ultimately keeping someone like Barry engaged with extreme content, in this case misogyny, that he would like, or follow, and would keep him on Facebook. It means they can sell more ads. It means more money. Facebook came back and said, "We prioritise communities over profit", but clearly this experiment, which was on a small scale, tells you at least something about how this works and where there are decisions not to deprioritise certain kinds of content, which to the broader public seems to be incredibly harmful.

Q137 **Simon Jupp:** How dark did it go in terms of the content that Barry was able to see?

Marianna Spring: A lot of the content was really disturbing. Lots of jokes about rape, harassment and sexual assault. There was a particular branch of the incel movement that had almost rebranded itself to seem a bit more palatable, using men's rights as a bit of a guise for some really extreme discussion of sexual violence, talk about rough sex, generally just really derogatory comments directed at women, and quite disturbing images and pictures. Even though I sort of expected it, it was astounding to see how quickly Barry was taken in by this world.

Again, to the Chair's point, it was not just English-language content. Some of that content was in Hindi, particularly from accounts originating in India. You see how this is universal. As we know, social media has no borders, and so a lot of this really awful content joins together, and you see how accounts are in some ways effectively radicalised by what they are seeing online. We have seen it with conspiracy theories and disinformation, and we see it with other forms of hate, in this case misogyny.

Q138 **Simon Jupp:** Forgive my ignorance on this question, but obviously the programme was broadcast a while ago. Do you know if many of those pages are still up; if that content is still around on those websites?

Marianna Spring: A lot of the content remains on those sites. Again, the response from the social media sites was very much, "We are committed to tackling hate. We try to not promote these kinds of content". We gave them the name of this account, they could look at the content it had liked, they could see what had been promoted to it and what it had engaged with. A lot of that remains.

That was another thing I found very surprising when we were doing this experiment, that that content even exists on their platform in the first place, those memes about rape, and sexual harassment, and sexual

violence are allowed, let alone that they are being pushed to users and that people are being sent towards this kind of content. It is not just about removing hateful content; it is about the role that these social media sites could play in making the problem worse.

Q139 **Giles Watling:** I too am interested in Barry. First of all, is he still alive? Is he still running?

Marianna Spring: No, he has ended his life.

Giles Watling: The experiment is over. There is no more Barry.

Marianna Spring: Sorry, that is a bit dark. His accounts have gone. He was suspended on Twitter.

Giles Watling: Really?

Marianna Spring: Only after we had flagged him.

Q140 **Giles Watling:** Extraordinary. Seyi mentioned earlier boys being corrupted in this way, but what fascinates me is the use of algorithms. In your experiment, Marianna, you instantly got responses. You put out that you like a certain page, and instantly you start getting responses. The point where you are buying a sofa, and suddenly you get loads of sofa advertisements, is it the case that young people, young boys, men even, become corrupted by algorithms? We are not talking about bad human actors here; it is because the algorithms are immediately pointing them towards these other sites.

Marianna Spring: Particularly in the case of the Barry experiment, because we began with Barry as a troll, the social media sites, like you say, recommend to you what you have already shown some kind of interest in. If you set up an account with no picture, with a very bland name, and did not engage in anything, you will most likely get recommendations based on where you live or the age you have given and the kinds of content they think you might like. What is crucial is that that experiment showed us that if an account shows an interest, even a small interest, in misogyny, the social media sites will inundate it with that kind of content. If, for instance, an account set up by a young boy starts to show some interest in a page with "I hate women" memes, suddenly they might find themselves, like Barry, two weeks later exposed to accounts that are joking about rape and sexual violence, with disturbing images. That is how it works. It is crucial, again, to come back to that commitment that the social media sites have made. We know this is how algorithms work. They promote content based on what you are interested in. That is not new, but they have said they tackle, and deal with, and forbid, effectively, online hate that is harmful to their users, and yet they are actively promoting it.

Q141 **Giles Watling:** What I am really trying to chase down is this old adage that the abused become the abusers. It is just possible, is it not, that somebody who might be suffering some abuse might click on something

online and then find they get inundated? Not setting up the site like you did with Barry, but they innocently click on something because they are subject to some abuse, perhaps offline abuse, and then suddenly they become the abusers. Is this a possibility?

Marianna Spring: It is a possibility. Because the algorithms detect what you are engaging with, if you engage in something along those lines you could very feasibly be promoted similar content that is disturbing, and extreme, and offensive, as Barry was. Another thing that struck me during the course of the investigation was I tracked down a number of the accounts that were sending me abuse, and back to the very original discussion about anonymity, a lot of them were not anonymous at all. It was very easy to figure out who they were, in fact. One of them was a man using his name and his image, and had five different Instagram accounts, all in that same name, all with that same image, and appeared to be hopping between them according to which one he was restricted from using. The social media sites tell us, again, as Twitter and Instagram did for "Panorama", that they make an effort to tackle accounts that are abusive. That does not mean they necessarily take them down. They can suspend them or sanction them in different ways. But again, this shows you that users work out how to get around that.

One of the accounts sending me abuse—not some of the worst abuse I get, which is one of the reasons I think he was willing to engage with me—was a guy called Steve from the Midlands, who is a van driver. I spoke to him on the phone. He began to realise, I think, the impact of sending gendered slurs and the kind of abuse that he had posted. What I thought was the saddest revelation of that conversation was that he said to me, "I sort of wish I did not really use Facebook. I can kind of see how I have ended up here". He was quite nice on the phone, and it was really sad. He has become very involved in anti-vaccine content and conspiracy content. He now thinks that global warming is not real. He thinks climate change is not real. He keeps sending me stuff about it.

Again, it is like I was saying before, there is a two-fold harm to this. It is about the women who are targeted with abuse and the kind of disturbing content that can embolden these kinds of trolls, that can lead to them receiving more hate that overall is harmful to them. But it is also about the Barrys and the duty of care to these people who are getting sucked into these very extreme and disturbing ideologies and are behaving in a totally disinhibited way, which has something to do with the way social media works.

Q142 **Giles Watling:** You are saying social media is fundamentally creating abuse. I want to finish by asking whether you think this legislation is dealing with that aspect.

Marianna Spring: I am here to talk about my reporting, and I defer to you as legislators in terms of what you say. But I do think "create" is the wrong word. I favour "worsening" or "making worse". I do not think "create" is necessarily wrong, but I have the evidence when it comes to

"worse", and I do not necessarily have the evidence when it comes to "create".

Q143 **Giles Watling:** Maria, can I put that to you?

Mrs Maria Miller: Yes. I will come back to your other point; the lack of regulation online is not benign. The fact that an individual can view something is not benign. It will change their behaviour. There is a lot of evidence to suggest that. I will go back to a slightly quiet piece of research the Government brought out that clearly shows the link between viewing extreme pornography, which is now much more available, and perpetrating domestic abuse. You are absolutely right, viewing something will then lead to a change in behaviour. Viewing something extreme will lead to a change in behaviour. On one level, this Bill does a great deal, because bringing in a duty of care will inevitably lead to a situation where at some point someone has to twig to the fact that extreme pornography, which will be unlawful offline, should now be unlawful online. That is a whole other kettle of fish I am sure the Committee will look at.

Also, going back to the issue of safety by design, algorithms should also be safe by design and should not do what Marianna has been talking about, pushing people into activities that are not only harmful but also potentially unlawful. There is a great deal in what you are raising there. When it comes to algorithms, the Bill needs to go further and be explicit on how it will ensure that those algorithms are also safe by design and how the duty of care will be brought to life by Ofcom in relation to the algorithms themselves. Ultimately, I see from having gone and seen how these operations work, a lot of it is to do with the cost of manpower moderating this manually. I suspect that if you require a great deal more personnel to moderate it could undermine the business model of many of these social media organisations, with devastating consequences for their share prices, as well, no doubt.

Cordelia O'Sullivan: Chair, may I comment on algorithms? One of the recommendations that we agree with is investing in more human moderators. A telling example when it comes to survivors of domestic abuse, one of the issues we face constantly, is perpetrators sharing content either directly or indirectly with survivors, which, on the face of it, appears absolutely fine, but against the context of domestic abuse and coercive control is deeply distressing. For example, images of her front door or street sign. Obviously when you understand that context, it is deeply threatening.

Chair: MPs suffer the same thing; I can tell you that now. I know that, because I have had MPs have exactly the same experience. They refuse to take it down.

Cordelia O'Sullivan: Absolutely. That is a massive issue, because that is something that is very unlikely for algorithms to pick up. You rely on victims reporting this and then going into extreme levels of detail as to why this is so problematic. A survivor who experienced something similar

said she was in a really dark place, constantly posting stuff, had really bad anxiety, panic attacks, and she was in the position where, if it was not for the tech abuse team, wanted to end her life because of this sort of abuse. The platforms were simply not engaging and did not understand that context of coercive control. We really support investing in human moderators, as well as recognising online VAWG and tech abuse on the face of the Bill, and specific codes of practice developed with the regulator. That is where we can really expand on what domestic abuse content looks like online.

Q144 **Kevin Brennan:** We are running rather late, so I will try to be brief and try not to repeat anything we have said before. From the answer Cordelia just gave us, would you all agree that having more human moderators would be a positive thing? That is something I was going to ask about. Does anyone disagree?

Seyi Akiwowo: I do not disagree, but having greater numbers is not going to do anything. We had Facebook representatives in Parliament before the pandemic. Do you remember what life was like before the pandemic? They gave us assurances that they would give us more human moderators. It is not numbers we want now, it is the training, to make sure they understand the language, the cultural references, the regional dialects, and the slang. That is also really, really important. There is no point having human moderators who all have very conservative ideologies and very minimal beliefs around women's rights. That will not solve things.

Q145 **Kevin Brennan:** Quality as well as quantity is needed.

Marianna, on the journalistic aspect of this legislation, the Draft Bill contains duties to protect journalist content and the content of democratic importance. As a journalist looking at this, are you concerned that this focus on protecting journalistic content might neglect the experience of prominent women in society in dealing with abuse and the long-term effects this might have? What is your judgment on what the Bill says there?

Marianna Spring: When it comes to the online abuse that I experience, again, I am hardly alone in terms of journalists who work at the BBC with me, who work across the media, but also particularly women journalists, and particularly black and south-Asian women journalists, or women journalists who are gay, or who are part of the LGBTQ+ community, who experience really awful hate day in and day out for doing their jobs. It is seen as part and parcel of being in public life. The problem is when it starts to affect your ability to do your reporting or to do your job. For me that is covering the evolution of anti-vaccine tactics that have become increasingly aggressive offline. Being able to report on that is crucially important to my job at the BBC, and if I am not protected from the kind of online hate that I experience when I do that reporting, it gets in the way of doing that. I think specifically it is important that women

journalists are protected in terms of the online abuse that they experience.

Q146 **Kevin Brennan:** Do you think the Draft Bill should go further in acknowledging that, or do you think it has it right currently?

Marianna Spring: Again, I will refrain from giving recommendations, but just look on the reporting that I have done. It is something that women journalists across the board experience, and it is clearly different compared to their male colleagues in terms of the nature and the volume of abuse, and it is clearly worse when it intersects with other forms of discrimination. I think it is important that we address the issue of online abuse targeting journalists in general, as my reporting and my own experience stands testament to. But I also think that acknowledging the differences in that experience is crucial in being able to tackle it in an appropriate way, because certain journalists experience this more, and in a different way, and they need support in different ways. I am supported very well by the BBC, but as I spoke about in the "Panorama", I feel like the police and the social media sites have not taken seriously the kind of hate that I experience.

Q147 **Kevin Brennan:** Thank you. Finally, Maria, I was very interested in what you were saying about the criminal offence you would like to see introduced into the Bill. You referred to a Law Commission recommendation that we should outlaw the taking, making and sharing of intimate images as a criminal offence. Can you give that a bit more context and explain the context to that as a legal change? Or is the suggestion that any taking, for example, of an intimate image could become illegal, even where consent is involved, and so on?

Mrs Maria Miller: The longhand is: taking, making and sharing of intimate images and posting them online without consent. Obviously, no, individuals have freedom to take photos in private, although too often, particularly young women—I am talking about when the image would legally be classified as child abuse—are unaware and not told how those images can be used in the future. When we started down this trail more than a decade ago with the advent of phones like that, children were taking images that were unlawful and distributing them, and too often adults were willing to say this is part of a normal, healthy relationship. I think children should be much better educated on the potential implications, because those images are there for the rest of their lives. They do not go away. I would like to see the law changed so that if those images are taken and if they are shared without consent, particularly online, the law reflects the gravity of the impact of that offence.

Q148 **Kevin Brennan:** Could that also incorporate the points you were making about deep fakes and the new technology that enables these things?

Mrs Maria Miller: It is deliberately phrased to be a catch-all to hopefully future-proof the issue that Jane brought up earlier, against new ways that the tech industry invents to give people the opportunity to take

these sorts of images. The nudification tool is a form of deep fake, and I think the Committee should note that this particular form of deep fake is only aimed at women. Obviously when we think about the way our laws are drafted, when we are trying to stop things that particularly affect women and particularly affect people who are covered by the Equality Act, we should be taking this very seriously.

Kevin Brennan: I am sure the Committee will consider that as a possible recommendation.

Chair: That concludes our session today. Thank you, Seyi, Maria, Cordelia and Marianna for your evidence today. It has been most illuminating.