

Women and Equalities Committee

Oral evidence: Pornography and its impact on violence against women and girls, HC 87

Wednesday 22 June 2022

Ordered by the House of Commons to be published on 22 June 2022.

[Watch the meeting](#)

Members present: Caroline Nokes (Chair); Elliot Colburn; Dame Caroline Dinenage; Jackie Doyle-Price; Carolyn Harris; Kim Johnson; Bell Ribeiro-Addy.

Questions 1 - 81

Witnesses

[I](#): Adam Baxter, Director, Standards and Audience Protection Team, Ofcom; and Sheryl Willson, Principal Public Policy Team, Ofcom.

[II](#): Rachel Maclean MP, Parliamentary Under-Secretary of State (Minister for Safeguarding), Home Office; Chris Philp MP, Parliamentary Under-Secretary of State (Minister for Tech and Digital Economy), Department for Digital, Culture, Media and Sport; Orla MacRae, Deputy Director Online Regulations, Department for Digital, Culture, Media and Sport; and Christian Papaleontiou, Deputy Director of Tackling Child Sexual Abuse Unit, Home Office.

Examination of witnesses

Witnesses: Adam Baxter and Sheryl Willson.

Q1 Chair: Good afternoon, and welcome to this afternoon's Women and Equalities Committee, and our inquiry into pornography and its impact on violence against women and girls. Can I thank our two witnesses—Sheryl Willson, the principal in Ofcom's public policy team, and Adam Baxter, director in Ofcom's standards and audience protection? As is the usual format, the Committee will ask you questions in turn. If either of you have not had a particular question asked of you, but you wish to jump in, please just put your hand up to indicate and I will endeavour to bring you in at an appropriate moment.

Adam, can I start with you and just ask for a brief overview of the role that Ofcom currently have in regulating content, particularly content that contains pornography?

Adam Baxter: Absolutely. I lead the team that, on a day-to-day basis, regulates broadcasting of linear channels on radio, TV, and notified on-demand services. We have very tight restrictions and rules in place on pornography. Dealing with the linear TV and radio broadcasters first of all, there is an outright prohibition on so-called R18 certified material. By that, I mean the special category of material which the BBFC—the British Board of Film Classification—categorises as legal pornography, the content of which sexual arousal is the primary purpose, but is very much at the strong end, so we have an outright prohibition on that.

For content that is not quite as strong, but we would still class as content with the primary purpose of sexual arousal, we classify that as adult sex works, and we do allow it under very strict terms on channels behind mandatory access protection between the hours of 10 pm and 5.30 am. As you can see from that, the controls on pornographic material are quite tight in the broadcast area.

Just going very briefly to the on-demand space, we have restrictions in place that mean on-demand providers must ensure that content that we would class as pornography—content similar to that which I have just described, such as R18 or adult sex works 18—would only be available to people who can pass the age authentication that the providers put in place. It cannot be a question of, for instance, just simple age assurance, like ticking a box and saying, "Yeah, hey, I'm over 18." There have to be ways of proving age, such as passport checks, credit card checks, etc.

That is, broadly speaking, how pornography is dealt with. Obviously, the code, consistent with the whole framework of freedom of expression, which we have to take into account, does allow—if the context allows it—broadcast content that might refer to sexual matters. For example, it could be a sex education programme or a drama with a love scene, but obviously those forms of content cannot just be put out willy-nilly. Typically, with a drama it would be very much later in the schedule, post watershed, with



HOUSE OF COMMONS

warnings and other protections. That is a very headline explanation, but that is how we approach it in the broadcast and on-demand area.

Q2 Chair: Thank you. May I just ask something around the British Board of Film Classification R18? Is that the right standard to use for online porn as well as offline porn? Would that give Ofcom the ability to regulate online porn effectively, or does it need to be different?

Adam Baxter: I will turn to Sheryl in a moment, but what I would briefly say, by way of observation, is that we work very closely with the BBFC. We have a long-standing relationship over many years and, as I have just outlined, our rules in the broadcast space and the on-demand space refer to BBFC certifications, so we are very used to using those standards. Sheryl, would you like to deal with the question about the online aspect?

Sheryl Willson: I believe that the definition in the Bill takes a consistent approach. It is, obviously, for Government and Parliament to decide how that is defined and what should be tackled in the Bill. Under the online safety regime, we think that it will have a real impact particularly on preventing children from accessing porn due to the duties in the Bill.

Q3 Chair: Thank you. I think we would all agree, would we not, that our main objective is to protect children and young people? We heard evidence several weeks ago, particularly on search services. We shall use Google as an example, but other search services are available. How does Ofcom expect them to minimise the risk of users who are under 18 unexpectedly encountering priority illegal search content? How simple will that be, and what measures are you expecting the search services to put in place to prevent that from happening?

Sheryl Willson: We are aware of the debate in this area. In terms of what is expected of search services, that is something we are exploring further with DCMS. We are still looking into what can be expected of search services; we do not have any specific recommendations at this point.

Q4 Chair: Looking at the minimisation of risk, we want to reduce the chance of the under-18s encountering this sort of material. What level is an acceptable level of risk? Are we seeking no under-18s being able to access anything? What is the tolerance threshold?

Sheryl Willson: Under the Bill, commercial providers of pornography will have to have suitable systems in place to stop children normally encountering that content, so that would be forms of age assurance and age verification. The Bill is not explicit on what is acceptable and what is not acceptable, and it is probably the right approach to allow those companies the flexibility to decide what is best for their service. Obviously, Ofcom's codes and guidance will help to set out examples of good practice in that space.

In terms of protecting children from user-generated content, platforms will have to have systems and processes that protect children and stop them encountering primary priority content. We would not be surprised if



pornography was within that category as well. Ultimately, Ofcom will take a risk-based approach when it comes to monitoring and enforcing. We will take protection of children very seriously. When carrying out our functions, we have specific duties to consider the impact on children, and within our enforcement guidelines we have to specifically consider how we will take account of the impact on children, so it is definitely a priority area for Ofcom.

Chair: Thank you. Let's turn to Caroline Dinénage.

Q5 Dame Caroline Dinénage: Thank you very much, and welcome to both of you. Let me start by asking you about the challenges that lie ahead, particularly when we are talking about enforcement action against some of the porn platforms. We are talking about platforms that have a reputation for not being wildly over-enthusiastic about age verification restrictions. We are talking about platforms that can often be fairly obscure in their ownership arrangements and, indeed, their country of origin. This is complicated stuff, so we are really keen to hear to what extent Ofcom is up for the challenge of taking this enforcement action.

Sheryl Willson: Enforcement, particularly cross-border enforcement, will not be without its challenges. I do not think we can get away from that, but we do have a number of tools at our disposal within the Bill. We can obviously try and engage as much as possible and send information requests, which we can enforce against as appropriate. If we take enforcement action overseas, we can seek to enforce penalties or other remedies, depending on the jurisdiction involved. We can co-operate with overseas regulators as they emerge and where there is alignment of approaches. Ultimately, if nothing else is successful, the last resort is pursuing business disruption measures via the UK courts, which would include potentially blocking access and restricting third-party services from non-compliant services.

Dame Caroline Dinénage: Did you have anything to add to that, Adam?

Adam Baxter: All I would say, by way of observation, is that we have a lot of experience in the enforcement space with linear and on-demand. We have not had the need to take the high levels of enforcement action, like the different categories of statutory sanction that we have in our regulatory toolbox, but we have, in the past, been happy to impose six-figure sums on some of these pornographers who—I agree with you—can be not the most straightforward category of business to deal with. However, we are very used to holding these sorts of people to account and I can foresee, as Sheryl just indicated, that we will be able to do so going forward because of our wide expertise in this area.

Q6 Dame Caroline Dinénage: Thank you. How do you envisage this working in practice? Are you envisaging a kind of proactive approach to how you regulate the services? That is very much the feedback we have been getting—that, in order to do this, you are really going to have to go out there very proactively to track it down and enforce it. Is that what you



have in mind?

Sheryl Willson: It will probably be a mixture. We are looking to have supervisory engagement with the largest and most risky platforms in scope—having that sort of dedicated engagement so we can be on the front foot in identifying risks. With the big pool of smaller services, we are thinking about what we can do to educate and to ensure that they comply. We are also thinking about how we can triage risks that come into Ofcom, and ensure that once that risk comes in from the various different forms of intelligence that we will have, what we should do next—enforcement or something else.

Q7 Dame Caroline Dinenage: Some of the illegal content that is described in the Bill—things like rape porn—is already against the platforms’ terms of service, and yet it is very difficult to track and remove it. Could this material be removed without Ofcom taking that kind of proactive approach? What if it is hosted on one of the smaller platforms, where you are almost waiting for people to flag it with you before you can track it down?

Sheryl Willson: There will be so many platforms in scope that we cannot monitor everything that happens, but we will hopefully have good relationships with different user groups that can feed information in to us with particular groups of users and concerns. We will have super-complaints and things like that to give us information. We will have our own complaints that we receive, where we can monitor trends and emerging risks. This is not a content moderation scheme. As I say, this regime has to focus on systems and processes, and we think that that is the right approach because it will allow us to interrogate platform systems and ensure that they are addressing any concerns at the root of the problem, rather than trying to take a whack-a-mole approach afterwards.

Q8 Dame Caroline Dinenage: Equally, the platforms that pose the biggest challenge, and potentially the biggest workload for you, will be those that are smaller, and difficult to track down, and they will probably be not wildly over-excited about the prospect of being regulated. Do you envisage this is going to be incredibly resource-intensive in that respect?

Sheryl Willson: We will take a risk-based approach. We will not just be focusing on the big platforms. The big platforms, obviously, have the biggest reach and that is why we would focus there, but we will also focus on smaller platforms that present a high risk as they emerge and develop. At the outset of this regime, we will be undertaking Ofcom’s own risk assessment of the different types of services that are in the scope of the regime. That will allow us to research and understand where the risks are at the outset of the regime, and inform how we target our resources.

Adam Baxter: If it is helpful to the Committee, I think there is a really interesting crossover here from the broadcasting experience, because we tend to find that the most problematic services in terms of the really harmful incitement and hate speech content tend to be the very small, less



professional outfits. As well as being very used to engaging with those people and ensuring that we hold their feet to the fire, we think it is incredibly important that we do expend the resource on such services, because it ensures that we maintain confidence in the whole regulatory regime. I guess a similar sort of principle will be carried forward in our online duties.

Q9 Dame Caroline Dinanage: I think that is absolutely right, and we have seen how platforms can go from being unheard of to being viral overnight. We have seen it with completely harmless things like Wordle. That is more of an app, I know, but we have also seen it on much more sinister online platforms such as some of the social media interactive platforms in the wake of things like the Capitol Building experience in the States. What resource have you got that is going to enable you to be aware, mindful and able very swiftly to respond to those more sinister and fast-growing platforms?

Sheryl Willson: We are looking at how we can horizon scan and monitor, and that will take different forms. Some of that is just monitoring services that emerge and media, but also looking at what data we can collect. We have a whole research team. We have a lot of different tools at our disposal to ensure that we know what services are coming through. It will not just be when they come through that we will focus on them; we will focus on them as they are growing.

Q10 Dame Caroline Dinanage: Final question: will you be ready?

Sheryl Willson: Yes. We have been in a fortunate position to have been given funding for this preparatory stage, which has been so useful and allowed us to recruit. We have, I think, 150 people working on online safety at the moment, with another 150 to come. We are already carrying out research. We are already preparing for our first wave of consultations. Yes, we will definitely be ready. That said, we need to ensure that we do this correctly, that the regime is robust, and that it can withstand legal challenge, so we need to be careful in our approach as well.

Q11 Bell Ribeiro-Addy: I want to ask about some of the issues that might arise when you are looking into sites such as YouTube, TikTok and Snapchat. As Caroline has already touched on, some of these things are already against the platform's terms and services, but a lot of the time much of the onus is put on the individual to say whether or not they are age appropriate to watch certain things. Young people often find their way around it, as they are more technologically savvy than their parents and, for example, with YouTube you will be going on to the next video. How does Ofcom intend to regulate a service like that, especially when it comes to the idea that, if there is a particular issue, you might block some of the sites, which could then affect someone's income now that people are using platforms such as TikTok and YouTube for a source of income?

Sheryl Willson: The Bill has various duties for the protection of children. It is not necessarily about blocking them in all cases; it is about ensuring



HOUSE OF COMMONS

that they have an age-appropriate experience. The Bill requires porn providers to prevent children from normally accessing those sites, so that means having age verification in place. On the user-generated side, it is about platforms making sure that children are having an experience that is appropriate to their age. For primary priority content, which could include pornography, they will need to ensure that children cannot access that. There are differing duties within the Bill, so it will not necessarily be about stopping them using it.

- Q12 Bell Ribeiro-Addy:** Generally, I am really concerned about how labour-intensive it might be for Ofcom to regulate these types of services overall. You have said you have some funding, but how sustainable is that funding? Would Ofcom approve, for example, of having some sort of fund, which sites that put forward the most types of issues would pay into, thus allowing Ofcom to better regulate them by, for example, employing more staff to look at these issues?

Sheryl Willson: Ofcom agreed the funding on the basis of the Bill that was published last year, I believe. That funding will not take into account any changes in the scope that have happened during passage, so it might need to be revisited. In terms of having a central pool that funds Ofcom, we think it is for Government and Parliament to decide if that is appropriate.

- Q13 Jackie Doyle-Price:** Sheryl, under this new online safety regime, if someone was a victim of image-based sexual abuse—for example, rape porn—who should they report it to?

Sheryl Willson: Incidents of that nature are already covered by criminal law, so we would, obviously, hope that such a horrible event would be tackled by law enforcement in that way. If content that amounts to an illegal offence is present— Well, first of all platforms should be taking steps to ensure that illegal content is not on their site, and for priority offences they need to ensure that there are steps to stop users encountering that. They also need to have clear and accessible complaints procedures in place for people to complain about content, which is relevant here. If Ofcom found that a platform did not have the appropriate measures to tackle illegal content or that they did not have an appropriate complaints system that was operated effectively, we could take enforcement action and investigate it.

- Q14 Jackie Doyle-Price:** Ofcom would be able to intervene, notwithstanding the existing criminal law, but do I understand from your answer that we are essentially looking at a self-regulatory system, but one where Ofcom can take an enforcement action if they are not satisfied with how complaints are being handled by the host?

Sheryl Willson: I understand the argument there, but it is important to note that they must have complaints processes in place that are clear, accessible and effective for dealing with issues like that. Rather than looking at any individual instances that might happen—which, of course,



HOUSE OF COMMONS

we would think are very serious and take seriously—Ofcom's focus will be on whether or not the complaints process itself is effective.

- Q15 **Jackie Doyle-Price:** Will you be doing any kind of thematic work as a regulator to look at some of these platforms and providers to assess the robustness of their procedures and, perhaps more than anything else, the clarity of how to complain, which is probably the most important thing?

Sheryl Willson: It is quite early to lay out anything specific now, but I imagine that we would do things like that to make sure that we are promoting good practice. Once we have our guidance in place, we can advocate good compliance and push for positive changes.

- Q16 **Jackie Doyle-Price:** If you look at how other regulators operate, highlighting good practice and, essentially, pursuing things that ought to be captured in a good process. Would you envisage doing that?

Sheryl Willson: Complaints handling is a cross-sector area, so I think it would be remiss of us not to look at other areas and sectors.

- Q17 **Jackie Doyle-Price:** Would you name and shame those platforms, providers and hosts that were not complying with what you would see as a clear complaints process?

Sheryl Willson: Any formal enforcement action would be transparent, so companies with any formal action like that would be named. I do not think we would name and shame outside of formal action, but I can double check that.

- Q18 **Jackie Doyle-Price:** As you say, transparency is probably the best form of action, not least so that users can protect themselves by only using those platforms and host sites that do comply with good regulation. Is there anything else you would like to add in connection with this new regime?

Adam Baxter: No.

- Q19 **Chair:** Sheryl, you referred to a "clear, accessible and effective" complaints process. How are you going to judge that?

Sheryl Willson: In preparing to deliver the regime, we will have a full consultation on our codes and guidance in all areas. Ahead of that, we will do our own work to establish good practice across the board. For example, you mentioned looking at other sectors. Then we will set out in our consultation document what we think is good practice, what the providers can do to comply. That will be a full, open public consultation. We would be keen to hear contributions from experts in the space, and then will publish our final guidance, which is what companies will have to look at and comply with.

- Q20 **Chair:** You said, "experts in the space." Are there any other stakeholder groups that you think it is important to consult with?



HOUSE OF COMMONS

Sheryl Willson: We engage with other regulators and international regulators. We will engage with user groups, civil society, charities, and platforms themselves.

Q21 **Chair:** Are you anticipating any particular engagement with groups representing disabled people or people with learning difficulties?

Sheryl Willson: I do not know exactly, but we definitely have a clear, structured plan in place to engage with user groups and charities that represent different groups of users that have particular needs. We are obviously very aware of the need to ensure that the more vulnerable groups are protected.

Chair: Thank you very much. Do any other Members of the Committee have anything further they wish to ask? Kim.

Q22 **Kim Johnson:** Good afternoon, panel. Sheryl, I would like to know how frequently you engage with some of these groups that you have just mentioned and how you do that. Is it online or face to face?

Sheryl Willson: I believe it is a mixture. I cannot give you a precise number, because I am not closely involved. If you would like some further information, we can follow up.

Q23 **Kim Johnson:** Final question: you mentioned earlier that you have 150 people currently working, with a further 150 being recruited. Out of those 150 that you have at the moment, how many cases would they deal with on, say, a weekly or monthly basis?

Sheryl Willson: At the moment, we are focusing on the implementation phase of the regime. We have 150 people working on the full programme of work, including programme management, research, developing our policy position, engaging with Government to support the Bill, and engaging with other stakeholders to gain understanding and develop our approach. It is not so much that we are looking at cases at the moment, but that is what we will be preparing for.

Q24 **Kim Johnson:** Do you have a deadline for that, Sheryl?

Sheryl Willson: In terms of implementation, we are somewhat led by parliamentary timelines, but we are planning on publishing our first wave of consultation shortly after we receive formal powers, after Royal Assent. That will cover the first wave of documents that we need for the first phase of the regime, which is around illegal content.

Chair: Thank you very much. Thank you both for your contributions this afternoon. We would appreciate some additional information on how you are going to consult and who with. That would be very helpful for us to understand the breadth of the consultation. I am going to suspend the meeting for a few minutes so that we can bring in our next panel of witnesses.

Examination of witnesses

Witnesses: Rachel Maclean, Chris Philp, Orla MacRae and Christian Papaleontiou.

Chair: May I thank our witnesses for attending this afternoon's session, as our second panel as part of our inquiry into the impact of pornography on violence against women and girls? I am going to turn straight to Carolyn Harris to ask the first set of questions, please.

Q25 Carolyn Harris: Thank you, Chair. My question is to Minister Philp. The Committee wrote to you on 13 June—I believe Minister Maclean was copied into that—with three specific recommendations for changing the Online Safety Bill. They were: age of consent checks for pornography uploaded online; basing the criminalisation of cyber-flashing on a lack of consent, not motive; and minimum standards for age assurance. What is your assessment of each of those recommendations?

Chris Philp: Thank you, Chair, for the invitation to appear before your Committee this afternoon. We are grateful for this opportunity. Thank you, Carolyn, for your question as well.

Just before I go into the specifics on those three points in the Chair's letter, it is worth just letting the Committee know that we are about two-thirds of the way through Committee at the moment discussing some of the issues that Carolyn touched on just a moment ago. I just want to make the point in introducing my answer that we feel this is a landmark piece of legislation. No other country in the world has yet regulated online services for user-generated content in the way that this Bill does, because it will, in particular, place an obligation on large social media platforms, such as Facebook and so on, to proactively prevent priority illegal content—the victims of much of which are women and girls—from being disseminated. We think this will have a huge impact in the area that this Committee will be concerned about. This is a huge step forward for women's and girls' safety in the United Kingdom.

Let me just turn, if I may, to the three points that appeared in the Chair's letter. Perhaps I could start with the question about age assurance. The Bill as drafted has a requirement on these companies—companies of any size, not just the big ones—where children in significant numbers may encounter content to ensure that children do not encounter the priority harmful material. The face of the Bill says that the measures that can be taken to implement that requirement can include age verification.

Just to clarify, age assurance is a general term that refers to any number of measures that can check someone's age. The hardest version of age assurance is a subset called age verification, which is where you upload a document like a passport or a driving licence or something like that. There is a whole number of other measures, which could include facial recognition, pulling in data from other sources and all kinds of other ways of doing it. It could be a third-party database, for example.



HOUSE OF COMMONS

The Bill works by saying they must take steps to prevent people who are under 18 from encountering this content, so pornography is going to be one obvious example of that. It specifies that age verification—the hard-edged version—is one way of achieving it, but Ofcom will then specify in codes of practice what other ways might be appropriate because the age verification version is quite onerous, having to upload passports and things, and some people might not want to do that.

Ofcom will specify in codes of practice other ways of achieving that same objective, which can include references to third-party technical standards. In facial recognition, for example, there is obviously an error rate, so you have to be careful about what is good enough and what is not good enough. That is a really deep technical standard that we would not expect in primary legislation. We would not necessarily expect Ofcom to specify it in codes of practice, but it might in its codes of practice refer to third-party technical standards generated by a standards institute—the BSI or somebody—or, indeed, academic standards that can then be applied.

The critical thing in this area, as in others, is that the duty is legally binding. The duty in this example is to stop children seeing pornography, so that duty must be delivered. If it is not delivered—as in, if children do systemically see pornography on a particular site—Ofcom can enforce against that. The codes of practice specify a way in which that duty can be met. A platform may try to meet the duty another way, but that only meets the duty if it is effective. If a platform says, “Well, we’ve seen this code of practice, and we think we’ve got a better way of doing it, so we’re going to do our own thing,” that is only adequate if Ofcom judge that it delivers the duty. If it is a rubbish way of doing it and it does not work, Ofcom will be able to enforce. Ofcom’s enforcement powers—this applies not just to age assurance, but to all the Bill’s duties—are extremely strong. They apply to everything we are going to talk about, so I will just say it now and it applies universally.

In terms of enforcement powers, in relation to information duties—where a platform like Facebook has to provide information to Ofcom—there is personal criminal liability. If a named executive or a senior executive is in a business that has not provided information requested, has obstructed Ofcom, has destroyed information, has lied to Ofcom or has otherwise prevented them from getting hold of the information it needs to work out what is going on, they will be personally criminally liable, with a prison sentence of up to two years. That is very important because we have seen other cases where these big platforms have refused to provide regulators with information and just paid a fine.

There was a Competition and Markets Authority case a year or two ago where one of these big platforms was repeatedly asked over a one-and-a-half-year period to provide information, refused to do so and just paid the £50 million fine. There is personal criminal liability for information provision.



Beyond that, there is the ability for Ofcom to fine these companies up to 10% of their global revenue, which can obviously run into billions. Ten per cent. of their global revenue is typically about 100% of their UK revenue. It varies by platform, but, as a rule of thumb, the UK is normally about 10% of their global market. In addition to that, in extremis, there are powers—denial of service and denial of access powers—where if they really do not comply after repeated asking, and after fines and everything else, Ofcom can basically have them disconnected from the internet: denial of service, denial of access, disconnected from the internet and disconnected from the payment system. The enforcement powers here are very strong indeed.

Q26 **Carolyn Harris:** Minister, how is that policed?

Chris Philp: Ofcom are the regulator, and it is Ofcom's job to watch what these companies are doing and if they are—on a systemic basis, not on an individual infringement basis—failing to deliver their duties, Ofcom will start using the measures that I have just described. There is also a mechanism in the Bill to raise a super-complaint. A group—for example, the NSPCC or someone representing a particular group of people, which in that case would be children—could be designated by regulations to raise super-complaints, and if they think there is a systemic issue that Ofcom has not noticed or has failed to act properly on, they can raise that as a super-complaint, which forces Ofcom to look at it.

Q27 **Carolyn Harris:** Is the onus, then, on complaints rather than Ofcom trawling on a regular basis?

Chris Philp: No, we expect Ofcom to proactively be policing the way that this is done.

Carolyn Harris: With the best will in the world, there are a lot of sites out there. It is very difficult to police all those sites to the extreme that you are talking about.

Chris Philp: If they miss anything, we would expect the super-complaint process to help, but obviously individuals can alert Ofcom to things. Ofcom are not going to act as an ombudsman on individual cases, but if they get a number of individual complaints about company X, I would expect Ofcom to think, "Hang on a sec, we've just had 20 complaints about this company, they all look similar, so we'd better do something about this." The responsiveness to super complaints will be a statutory duty, but I would also expect them to be, as a matter of common sense, responsive to individual issues if they are raised to the point that they think there is a concern.

Q28 **Carolyn Harris:** What is the benchmark for complaints for Ofcom to intervene?

Chris Philp: If it is a super-complaint, it is like any super-complaint that meets the statutory test, which is set out here and we went through in detail in the Committee—clause 140 in the Bill. We are obviously getting



into a specific thing here, but it is worth doing because it applies to everything. In order to qualify as a super-complaint, it has to be systemic and significant. The test is that it needs to: cause “significant harm to users of the services or members of the public”; significantly adversely affect “the right to freedom of expression” etc; or have “a significant adverse impact on users of the service or members of the public, or on a particular group of such users or members of the public”, which could obviously include children, women, minorities or whatever it may be.

There will be these designated organisations like the NSPCC—I do not want to prejudice the decision, but they would be an obvious one—that will be able to raise these super-complaints. In the next clause, the Secretary of State will make regulations to specify things like a timeframe for replying. Replying to these super-complaints is not optional; Ofcom have to do it.

Orla MacRae: Ofcom in general will need to take a risk-based and proportionate approach because, as you say, there will be many companies in scope, and they cannot possibly be actively looking into each one. Pivotal to that is the requirement in the Bill for Ofcom to do a risk assessment. This is one of the very first things that will happen under the Bill. Early on after Royal Assent, they will need to be looking across the landscape of the sector and the different companies to identify where the greatest risks of harm to users fall, and that will give them the starting point for where they pay most attention. Obviously, they will need to flex that, as the Minister says, in response to new information coming in through the complaints.

Q29 **Carolyn Harris:** Minister Philp, although services must restrict children’s access to both, the Bill currently subjects user-generated porn but not provider porn to the safety duties under part 3. Can you explain why that is the case?

Chris Philp: I would be happy to, but I have only answered one of your three questions.

Carolyn Harris: Oh, right, sorry.

Chair: I am sorry, but you are going to have to give much shorter answers.

Chris Philp: I apologise. I have become habituated to speaking in Bill Committee where—

Chair: You are using up time.

Chris Philp: I am sorry; it is not intentional. Do you want me to try and answer those other two points or?

Chair: Yes, but snappily.

Chris Philp: One of the questions was on clause 156, which is basically cyber-flashing and whether the threshold—the trigger—should be consent or intent. We followed the Law Commission’s recommendations because they are the experts and the test is that there needs to be an intention.



This is the cyber-flashing offence. There needs to be an intention to cause “alarm, distress or humiliation”, or the image is sent for the purpose of “obtaining sexual gratification” and there is recklessness as to whether the recipient is caused alarm, distress or humiliation.

Clearly, that is a slightly higher threshold—intent, rather than simple absence of consent. Very often the context will make the intent clear. The use of the intent test does follow the offline, existing traditional indecent exposure offence in the physical world. That is why we have cast it as it has been cast following Law Commission advice. Maria Miller asked some very thoughtful questions about this in Bill Committee yesterday, and we are doing a bit of further thought about whether this can be further improved.

Chair: Can I just interrupt you because two Members want to come in on that point. I very much welcome the comments you made yesterday about looking at further thought around that. I think this entire Committee would be interested in where those further thoughts go. Jackie?

Q30 **Jackie Doyle-Price:** Can I just ask Rachel Maclean what your views are on that? If this Government are serious about tackling violence against women and girls, which I believe you are, surely consent should be the criteria, not the intent of the person. We really have to level up the impact on the victims of these crimes.

Rachel Maclean: Thank you for inviting me here as well. Jackie, you are absolutely right; of course we take it seriously. It is one of the huge priorities of the Government. That is why we have published the violence against women and girls strategy. It is a very comprehensive strategy which covers a huge number of areas, and how we will improve the response to violence against so many girls across law enforcement, society, education—

Chair: We know that, Rachel. Answer the question please.

Rachel Maclean: Can I just caveat this, please, Chair? It is quite important to know this. All these offence issues are an MOJ lead. I need to make that point very clear. The actual decisions on what is and what is not an offence are not for me. Obviously, I have a view. You asked me for my view and I am going to give it to you. My view is that, as Chris has said, we need to take the Law Commission’s steer. That is a standard practice across Government because they are the experts, and anybody here will know that we are duty bound not to introduce superfluous offences onto the statute book.

There are some real questions over this. We are introducing a cyber-flashing offence. I have had this discussion separately with Maria Miller and I understand why she says what she says. We have to look at the balance between over-criminalising—I think over-criminalising is a genuine concern—and capturing those people who are obviously sending these horrible images. We know that these images have a devastating impact on



HOUSE OF COMMONS

many girls, but we do not want to over-criminalise people who just might be doing something between two consenting adults, for example. Now, I appreciate this is a balance, and I do not pretend to be—

Q31 Jackie Doyle-Price: No, it is not a balance. If you are serious about tackling violence against women and girls, we should be centring women and girls. One of the reasons why we are pushing relationships and sex education so early in schools is to teach girls to be empowered and for them to recognise that it is up to them to give consent. That should be running throughout the whole law, surely.

Rachel Maclean: I think it does. We are talking about one specific point, and, as I said at the beginning, I am not a legal expert; I am not the one who is leading on the legal provisions. What you are challenging me on is the intent here. Are we protecting women and girls? I would argue that, yes, we are because we are bringing in a wholly new offence that did not exist before, alongside a number of other new offences, such as false communications, the whole intimate image abuse communications and some of the deepfake issues. These are all being brought in with this Bill. We are absolutely looking to protect women and girls from the sorts of things that you are describing, but I have to accept the legal experts when they say there is a genuine risk of over-criminalising images that are innocent in some shape or form.

Jackie Doyle-Price: I suspect they are men, but—

Rachel Maclean: Minister Philp has said he is going to look at this again, and I am sure he will have looked at this in an extreme amount of detail in the Bill Committee.

Chris Philp: Rachel is right; this is an MOJ lead. Just two points: this cyber-stalking offence is brand new; it did not exist until this Bill introduced it, and everyone yesterday in the Committee, including the Labour Front Bench, accepted that it is a massive step forward. I think I am right in saying that the intimate image abuse offence, which again is an MOJ lead that they are currently working on with the Law Commission, is consent-based, which will give another avenue to pursue.

Q32 Elliot Colburn: Minister Philp, can I just press you a little bit more on intent versus consent? For clarity's sake, could you confirm if the onus of proof would be on the plaintiff or on the defendant in a cyber-flashing case? Would it be on the plaintiff to prove it or on the defendant?

Chris Philp: It will be a criminal prosecution so there is no plaintiff; it is the CPS that will be prosecuting the offence. As with any criminal offence, the burden of proof sits with the prosecution to establish beyond reasonable doubt that the offence is made out. Establishing the intent to cause alarm, distress or humiliation, given the context of many of these totally outrageous pictures that get sent around, will be very persuasive in helping the CPS to establish its case to the required standard.

Q33 Elliot Colburn: Would it not be safer to have an offence based on consent?



I totally appreciate the point that Minister Maclean made around over-criminalisation and perhaps unintended consequences, but would it not be safer to have an offence based on consent with defences based on intention?

Chris Philp: With defences based on intention? You could, obviously, frame it that way. As I said, Maria Miller had some thoughtful points to make about this in a speech that she gave to the Bill Committee yesterday, which we are looking at. That was not one of them. We would be happy to give that some thought. As Rachel said, this is a very delicate area. Our starting point is always the Law Commission recommendations, because they have studied this quite deeply.

I have had some lobbying from colleagues in Parliament who, before they realised it had the intent qualifier, were concerned that if we put consent in here, people who knew each other very well, or who were on certain kinds of dating websites and habitually might exchange these images without express consent but either in a relationship or in an online environment where the exchange of those kind of images was generally considered fine, that might criminalise those kinds of exchanges. There are some sensitivities to think carefully about to avoid over-criminalisation.

Q34 **Chair:** Can I ask what regard you have given to the victim in those considerations? We have a victims Bill in front of Parliament at the moment, and the failure to include consent disregards the impact on the victim.

Chris Philp: Most criminal offences do have a mens rea component, which is to say that the perpetrator has to intend to commit the offence. Where you have a purely consent-based offence, one is departing from the general approach that the criminal law has taken for hundreds of years. To be clear about the victim, the test is whether the intention is established to cause alarm, distress or humiliation to and of the victim. The impact on the victim is right there; it is their alarm, distress or humiliation that is at issue.

Q35 **Chair:** It is quite hard to send an indecent unsolicited image accidentally, is it not?

Orla MacRae: The Law Commission looked at some very innocuous things as part of its consultation—for example, a photo on a beach where there is a nudist sunbather behind the person, in the background, and they send that image to someone, and because it has that naked person behind them, that might inadvertently be criminalised. The other example is around young people, who maybe do not have the maturity to make some of these judgments, being over-criminalised for misjudgements in their youth, which the Law Commission advised would be disproportionate.

Jackie Doyle-Price: There is still a victim there.

Orla MacRae: If someone receives a photo of a nudist?

Jackie Doyle-Price: If someone is a youth, there is still a victim.



HOUSE OF COMMONS

Chris Philp: That is true, there is; you are right, Jackie. The question is whether the person sending it should be criminalised and potentially sent to prison for a couple of years, if they did not intend to commit an offence.

Chair: Normally the CPS would not prosecute that because there would be no public interest in it.

Chris Philp: They have to prosecute what the law says.

Chair: They do not prosecute rape.

Rachel Maclean: That is a separate discussion, which I am very happy to come to the Committee—

Chair: No sorry; that was a flippant comment, Minister.

Rachel Maclean: They actually do prosecute rape. We have made some very good progress on that, and I would actually be delighted to come to your Committee and talk about that.

Chair: Carolyn, can we go back to you?

Q36 **Carolyn Harris:** Minister Philp, we have been talking about victims, and I want to talk about rape porn. One of the witnesses we heard stated that there was more concern over the content than the access. There was far more concern over what was on there than over people being able to access it easily. What do you see Ofcom being able to do in order to stop this illegal content being so available?

Chris Philp: It is a really good question. The most powerful duties in this Bill—binding companies of all sizes, not just the very big ones—are the category of content that we are calling priority illegal content. It is listed in schedules 6 and 7 to the Bill. For the criminal offences on that list, the search engines and social media firms have to proactively seek to prevent this content from being uploaded and disseminated. The schedule 6 priority offences are basically all to do with child sexual exploitation, as you would expect. There are also terrorism offences in schedule 5, which are also priority offences.

Then you come to schedule 7. Many of the priority offences, where the platforms have to proactively take steps to stop this stuff, are things that women and girls disproportionately suffer from. They include things like: “fear or provocation of violence”; “intentional harassment, alarm or distress”; the stalking offences—stalking involving fear of violence offence—

Q37 **Carolyn Harris:** Minister Philp, can I just take you back to what I said earlier: who polices that and makes the decision as to whether the victim feels intimidated? Surely it just being there victimises them anyway, and there should not be a decision of whether we should prosecute; they should be prosecuted.



HOUSE OF COMMONS

Chris Philp: Ofcom's work in policing this and the platforms' duties apply whether or not there is a prosecution. The criminal prosecution is a separate thing for the police and the Crown Prosecution Service. Essentially, if there is content online that you might reasonably assume amounts to that offence, regardless of whether it has been prosecuted, these duties apply. If there is content on there that amounts to any of these things, they have to proactively stop it.

Q38 **Carolyn Harris:** Is that dependent on an identifiable victim? If the victim is not identified—

Orla MacRae: What is probably important to add is what has to happen under the Bill is that each company in scope will take that list of priority offences and do their own risk assessment to think about the risk of that type of content appearing, and then they have to put in place proportionate systems and processes to manage it. It sounds very procedural, but—

Carolyn Harris: Effectively, they mark their own homework.

Orla MacRae: Not at all. Just to finish on what platforms have to do, the onus is on them to comply with their duties in the Bill, and it is Ofcom's role to make sure that what they are doing is sufficient to manage and mitigate the risks identified. That is going to be much more effective than a regime based on looking for individual pieces of content, because, as you have implied the scale is—

Chris Philp: But to be clear, there does not need to be an individual victim identified. If there is content that breaks one of these laws, even if no individual victim is identified, they still have to stop it.

Orla MacRae: Or stop the risk of it.

Chris Philp: They have to stop even the risk of it, yes.

Q39 **Chair:** Can I take you back, Minister Philp, to something that you said right at the beginning about children in significant numbers being able to access porn. Can you define significant for us?

Chris Philp: Are you talking about the child access condition?

Chair: Yes.

Chris Philp: That will be up to Ofcom to set out in their codes of practice. This is essentially a qualification used to decide which platforms are subject to the children's safety duties, which are the ones that basically say the platforms have to proactively keep children safe from the primary priority harms such as pornography and those sorts of things. Clearly, we would not want Ofcom to be getting involved in a website if, for example, one child stumbled across something, but there has to be some kind of threshold to make sure there they are concentrating their resources at the right levels, which is why the word "significant" is used.

Q40 **Chair:** What is it?



HOUSE OF COMMONS

Chris Philp: I cannot give you a number. I cannot tell you whether it is 10, 100 or 1,000. Essentially, it will be defined by Ofcom in their codes of practice. Obviously, it will be something they can vary in the codes if they decide over time that the threshold is set in the wrong place and they are missing harm, which is another reason for not setting it out in primary legislation. If we just put a number in, like 10,000 or 1,000, we might then find there are unintended consequences—either it creates a burden on Ofcom that is just unmeetable, or conversely it is set too high and real harm is missed. It is left somewhat flexible for Ofcom to implement, because we do not want to tie Ofcom's hands too much in primary legislation as we are not going to change this Bill for probably another five or 10 years.

Q41 **Chair:** What is more important, not giving Ofcom a target that is unmeetable—I cannot remember how you just described it—and overburdening Ofcom, or protecting children?

Chris Philp: Ofcom clearly has finite resources, as does every organisation in the world, and we want to make sure those resources are prioritised to the areas where they will have the most impact. This Bill is about trying to direct the platforms themselves, and Ofcom as the regulator, to the areas where there is the most harm, hence the priority illegal offences that I mentioned a minute ago, the measures on child sexual exploitation and the emphasis on terrorism. We want to make sure they direct their attention to the maximum areas of impact, which I believe is a fairly reasonable principle.

Q42 **Chair:** Another point you made is around age verification and people being asked to upload passports, and going through those funny experiences where you turn your head to one side and the other so it can verify it is you. We have all been through that for various websites. You said some people might not want to do that; I think we can understand some people may well not want to do that. Is their right to not want to do that more important than protecting children?

Chris Philp: Ultimately protecting children is the most important thing, but the point is that the onus is on the companies to demonstrate that their alternative method—facial recognition or whatever else—enables them to say it does the job; they have to prove it works. If it does not work and they cannot prove to Ofcom that whatever it is they are proposing is effective, the bottom line—the safety net—is age verification.

We made an amendment to this Bill following its initial publication to insert the words “age verification”—meaning the passport stuff—on to the face of the Bill to make it completely immune from legal challenge. If a company cannot prove they are meeting their duty some other way, they must use age verification.

Q43 **Chair:** If you talked to the Children's Commissioner, she would make the point that none of them want to do anything around age verification, but the porn companies would do it if required to by law. Is it not best to just



HOUSE OF COMMONS

start with that presumption of “Let’s have it as safe as we possibly can for our children”?

Chris Philp: The way the Bill is constructed is that it says they must meet the duty, which is to stop people under 18 seeing porn. If Ofcom can be shown a way that works that is not age verification, they can do that, but it must work. Otherwise, it is age verification. That is not an unreasonable approach, but we have put age verification on the face of the Bill, and it was not in the previous version, just to make sure there is no chance of legal challenge if some company says, “Well, that’s an unreasonable duty”. It is on the face of the Bill.

Q44 **Elliot Colburn:** Ministers, can I ask you both about the Online Safety Bill’s relation to violence against women and girls and the VAWG strategy? The Istanbul convention, that the UK is a signatory to, states that domestic laws need to take a gendered approach. Indeed, the Home Office’s own VAWG strategy does so, and yet the Online Safety Bill, which the VAWG strategy regularly refers to, does not mention gender once. Can you explain why that is? Minister Maclean, could I start with you?

Rachel Maclean: Violence against women and girls is, of course, a priority, as you know and as you have agreed. What we are talking about here is a mechanism of enforcement. It will be for Minister Philp and DCMS to talk about the language that is in the Bill. But does it deal with our obligations under the Istanbul convention? Yes, it absolutely does, because it introduces a lot of new protections for women and girls to keep them safe online, whereas hitherto they were at risk of all sorts of threats, risks and harm.

We are bringing the online environment in line with the offline environment. We have already made a lot of progress in that space, and this Bill will enable us to do that. I do not know whether Minister Philp can come back on that particular point about gender in the language of the Bill?

Chris Philp: I am not sure if the members of the Committee have the Bill in front of them—I seem to be rarely separated from it these days—but in terms of gender in the Bill, the risk assessment duties are the starting point for the whole architecture of the Bill. You have to do your risk assessment and then make sure you deal with the risk identified. There are two places in the Bill where the risk assessments refer to “characteristics”, meaning gender, ethnicity, sexual orientation and so on. For the benefit of the Clerk, if they want to check this later, it appears in clause 10(6)(d) on page 9 in the children’s risk assessment duties, so the risk assessments have to look at the characteristics of the children—gender, race and so on.

Q45 **Elliot Colburn:** Sorry to interrupt you Minister, but when you say “characteristics”, are we talking about the same protected characteristics within the Equality Act? Do they mean the same thing, or is this a different version of the word?



Chris Philp: It could be broader, but it certainly includes all the characteristics under the Equality Act.

Q46 **Chair:** How could it be broader?

Chris Philp: There could be other characteristics that are not the protected characteristics in the Equality Act.

Chair: Like?

Chris Philp: I do not have the list in front of me, so I do not know, but it is not limited to the Equality Act protected characteristics. It occurs again in relation to the adult risk assessment duties in clause 12(5)(d) on page 12, with the same reference to characteristics. The risk assessments have to account for additional vulnerabilities or risks that attach to people with characteristics, such as ethnic minorities being at risk of racial abuse, women and girls being at risk of misogyny and gender-based abuse, and so on. It starts right there in those risk assessments.

Q47 **Elliot Colburn:** Thank you for that, Minister. Just to play devil's advocate a little bit, if the Bill were to contain gendered language, would that present a risk in terms of potentially excluding some people from being considered victims under the Online Safety Act? Let me give you an example that might help to clarify what I am saying. If the Bill had gendered language, and we were talking about cyber-flashing as the specific offence, let us take the approach of someone using AirDrop to send indecent images to the people in their immediate space. You have no idea, obviously, of the gender of the people you are AirDropping an image to. Would gendering the Online Safety Bill present a risk that male victims of cyber-flashing may be excluded from being a victim of the offence?

Orla MacRae: If you added the reference into the criminal offence so you limited cyber-flashing to women and girl victims, that would obviously exclude men from benefiting from those protections. That is a slightly different point from the wider regulatory framework, where we think it is already very much baked in that companies need to consider all the various different characteristics of their users.

Chris Philp: There are two different points here. One is considering the risks that are particular to certain groups, like ethnic minorities, women, girls, etc. The risk assessments need to reflect the fact that some of those groups, like women, are much more at risk than other groups, like men. But in terms of the actual criminal offences, I agree with your point that you would not want to inadvertently exclude certain victims. Most, if not all, of the criminal offences currently on the statute books, including ones that are essentially designed to protect women, like stalking, are not gendered as they are currently written.

Christian Papaleontiou: That is correct, it would be in breach of the Equality Act if they were. *[Interruption.]*

Chair: We do not need any answers from the PPS, thank you. You are not



HOUSE OF COMMONS

part of the panel.

Chris Philp: He is very good.

Chair: I am sure.

- Q48 **Elliot Colburn:** You mentioned that although the Bill does not necessarily use the phrase “protected characteristics” in the same way that the Equality Act does, the Bill is not limited to those characteristics and could go further. Again playing devil’s advocate, by equal measure could that mean that it is also not restrained by them and could go backwards?

Chris Philp: Can you explain that a bit more? I did not understand.

- Q49 **Elliot Colburn:** You have mentioned that they are not the same protected characteristics as defined in the Equality Act. Therefore, does Ofcom have the ability to define characteristics in an entirely different way from the definition in the Equality Act and decide that one of those nine is not as in need of protecting as another?

Chris Philp: Given we have this well-established list in the Equality Act of protected characteristics that have been established for 12 years now, and are kind of universally accepted, I would be very surprised if that did not form the basis of this, but there may be other characteristics that get added in the future.

Orla MacRae: Ofcom is a public body and as such is bound by the public sector equality duties, so it would be bound by that.

Chris Philp: This is the point. If Ofcom used only seven of those nine for example, and decided to arbitrarily or for any reason delete two of them, that probably would breach its own PSED as a public body.

- Q50 **Elliot Colburn:** Thank you, that is really reassuring. How do you expect Ofcom to go about producing a code of practice specifically pertaining to violence against women and girls, given that gender is not mentioned in the Bill?

Chris Philp: We would expect Ofcom to have regard to the research in this area. Gender is not in the Bill in itself, but there is reference to characteristics. As you have said, one of those characteristics is gender. As I read out those references a couple of minutes ago, I will not test the Chair’s patience any further by repeating them. Through those references to characteristics, gender has to be in the risk assessments, and would obviously then get assessed by Ofcom to determine whether they are adequate. In doing that, we expect Ofcom to draw on the range of relevant research, and there are various consultation duties.

Rachel Maclean: Can I add to that, Chair? It just might be helpful to the Committee to know that I have met some of the stakeholders who are calling for this code of practice for VAWG. We had a very good meeting with them, and I am sure that you have probably heard them in front of



HOUSE OF COMMONS

your Committee. In fact, one of the organisations has produced a VAWG code of practice.

We had a really good discussion with them, and were able to allay some of their concerns that what they wanted to be covered would be covered within the existing framework of the Bill. It is particularly important to make the point that even though the Bill is not gendered, as you rightly pointed out, a lot of the harms it is protecting against disproportionately affect women and girls already. Impacts of pornography, cyber-flashing, cyber-stalking, coercive control—all these things disproportionately affect women and girls.

We were able to alleviate some of their concerns, and also explain the way that Ofcom have a duty to address all of this, and the freedom and power that they have provides a duty on them to address it. Of course the mechanics of it are for Minister Philp, but Ofcom have that freedom, duty and requirement to address this, even though there is not necessarily a specific code of conduct for these issues.

Q51 Chair: Minister Maclean, thank you for that comment about the impacts of pornography. Can I just ask what research the Government have done to understand what impact pornography has on driving offender behaviour?

Rachel Maclean: You will probably know about a lot of this as well, Chair. The Government have looked into this specific issue, with research commissioned by the Government Equalities Office. It has not established a direct causal link between pornography and harmful sexual behaviour. This is one of those areas it is incredibly difficult to research and get any robust evidence in. Nevertheless, regardless of the fact that there is no evidence there, we clearly regard the viewing of pornography, extreme pornography, and those categories of pornography that the Bill will be dealing with, as incredibly harmful against women and girls.

Q52 Chair: When was the GEO research carried out?

Rachel Maclean: I am not sure if it was 2015. My officials may be able to—

Christian Papaleontiou: I was looking at this morning. It was published in 2020. We can send you a copy.

Rachel Maclean: Can I just add that we have more recently also commissioned a much broader piece of research from Bristol University, which looked into lots of different forms of the adult services industry, including webcamming etc. It is a very detailed report that I am happy to share with the Committee. Again, we cannot find evidence of robust causal links from this research, as you are suggesting.

Q53 Chair: What reflections did DCMS have on the GEO research when looking at the online safety legislation?



HOUSE OF COMMONS

Chris Philp: We are obviously very concerned about the impact that extreme pornography can have. That is one of the reasons why the Bill was amended when it was updated and introduced in February or March to include commercial pornography sites in the scope of the age gating duties, which was previously pointed to as a gap in the Bill. We were keen to make sure that people under 18 did not access that, because obviously—

Q54 **Chair:** Let me ask that in a more specific way: did you look at the GEO research?

Orla MacRae: It was actually published before the Minister joined the Department, but we worked closely with the Government Equalities Office on it and certainly did look at it when it was published.

Q55 **Chair:** Has DCMS also considered this newer research commissioned by the Home Office from Bristol University?

Orla MacRae: I am not aware that we have seen that research, but we certainly will.

Q56 **Elliot Colburn:** When did it come out?

Christian Papaleontiou: It was published last year, and again we can forward it. To be clear, the research from Bristol University was very much a piece of research into sex work and prostitution, which I know the Committee will want to ask further questions about later. Again, it touches on the fact of how sex work and prostitution has changed with the birth of the internet and the diversity—

Q57 **Chair:** Presumably that plays into what I would see as a rather unpleasant relationship between online pornography content that you might find on social media and then moving on to OnlyFans?

Rachel Maclean: I have it somewhere in my pack; it is a very long report.

Chair: I am sure.

Rachel Maclean: Yes, as you can imagine. It looks at all the different manifestations of sex work—where it occurs, the risks, the vulnerabilities, the different business models.

Q58 **Chair:** Were DCMS not aware of it? Have DCMS looked at it?

Rachel Maclean: It was a Home Office piece of research, and I am sure officials have seen it.

Orla MacRae: I should say the Online Safety Bill as a whole is a joint endeavour with the Home Office.

Q59 **Chair:** Okay, a specific question then: have you looked at it?

Orla MacRae: I have not personally seen it.

Q60 **Chair:** Has anyone in DCMS?



HOUSE OF COMMONS

Orla MacRae: I could not comment on behalf of the entire Department.

Chair: Maybe we could have some clarification on whether the Home Office has shared it, and whether we are having joined-up government on that. Kim.

Q61 **Kim Johnson:** Good afternoon, panel. Minister Maclean, if a woman or girl finds sexual images of themselves on pornographic sites that they did not consent to, what would be your advice to them?

Rachel Maclean: Are you talking about a cyber-flashing offence? I presume you are, because if they were—

Kim Johnson: Any kind of sexual images that might find of themselves on pornographic sites.

Rachel Maclean: Images of themselves without their consent?

Kim Johnson: Images of themselves without their consent.

Rachel Maclean: The Online Safety Bill requires the platforms to bring in mechanisms for them to report that, so I would expect them to look at what the provisions are within those platforms where they have seen that and report it.

Q62 **Kim Johnson:** The specific question was what would you advise them to do?

Rachel Maclean: I would advise them to report it immediately.

Q63 **Kim Johnson:** To the police or to the site?

Rachel Maclean: No, to the platform where they have seen it.

Q64 **Kim Johnson:** Is that a process you would say is quite easy to undertake?

Rachel Maclean: At the moment the process does not exist because the Bill has not been passed, but clearly when it is passed, it should absolutely be much easier than it is at the moment.

Q65 **Kim Johnson:** Some 77% of respondents to the Home Office victims and survivors survey reported that there was very little support available. What will the Home Office do to address these issues?

Rachel Maclean: You are right to say that presently it is very difficult to get support in the situation that you have mentioned, which is why we need this legislation and why it is so important because it does bring in much better protection and forms of redress. We are, of course, working closely with DCMS. We are here together, to make sure they have that support.

More broadly, we are funding support for victims of sexual violence, which is actually an initiative of the MOJ. There is a lot of support being invested as part of the latest spending announcements from the MOJ, which is linked to the violence against women and girls strategy, all the work that we are



HOUSE OF COMMONS

doing in the rape review space, and it links to all the funding that we are giving to ISVAs and IDVAs as well.

Christian Papaleontiou: The Home Office also funds the revenge pornography helpline and is committed to continuing the funding, which has been increased in this financial year. This is again a source of support, guidance and help for any woman or victim who has experienced this. There is then the issue of the response you get when you report to a company. At the minute it is not adequate, which is why we are bringing in the Online Safety Bill.

Q66 **Kim Johnson:** Are you monitoring and reviewing how well that service is being utilised at the moment?

Christian Papaleontiou: They will be subject to all the controls in terms of signing the grant and making sure we have returns. From memory, the number of calls that have gone to the revenge porn helpline has gone up to 16,000 victims they have helped. Let me just check that figure—it is in the pack.

Q67 **Kim Johnson:** Would the helpline triage people—women, whoever—to specific organisations for help and support?

Christian Papaleontiou: They will be able to provide direct support if they feel able to, or they can refer them to an alternative service if their needs are greater and more complex and they require further support from one of the organisations the Minister just referenced.

Chris Philp: Can I just add a couple of points? I have the helpline numbers here. Since it started operating in February 2015, it has helped 14,000 people—I presume, overwhelmingly women—and has seen the removal of 260,000 images.

Secondly, it is obviously a criminal offence now under the revenge porn offence in section 33 of the Criminal Justice and Courts Act 2015. If a woman, or anyone, is the subject of this, they should report it to the police because it is a criminal offence.

The third point I would make it about reporting to the company to get it taken down. At the moment, this is very patchy at best. People say they report stuff and nothing happens. One of the statutory requirements in this Bill is for these bigger companies to have a proper process for reporting this sort of thing and other complaints. It has to be accessible to people, including children, and they must respond in a reasonable and timely manner. If they do not do that, Ofcom will enforce against them.

Your question basically has three answers: revenge porn helpline; police; and the companies who, following passage of this Bill, will have to run a proper complaints process, which quite frankly they do not at the moment.

Q68 **Kim Johnson:** Thanks, Minister, that moves us quite nicely on to my second question to you. Would Ofcom be able to intervene if the host



pornographic site refused to remove non-consensual sexual material when asked by a victim, including through the police?

Chris Philp: On a systemic basis, yes.

Q69 **Chair:** Thank you. We heard from Ofcom earlier about the complaints process that had to be clear, accessible and effective, but they were not particularly keen to quantify that—to say how accessible, clear and effective it is. Minister Maclean, I will start with you. What do you think clear, accessible and effective looks like, and how quickly do you think companies should be able to respond?

Rachel Maclean: As you have already touched on in your questioning, it should be instant and should provide reassurance for women and girls, or anybody who sees images of themselves or other offensive images to get redress. It should involve it being taken down, because sometimes—to be clear—these images are dangerous. Often in a situation of domestic abuse, for example, if a perpetrator is posting pictures of a woman in certain situations, that can constitute a very dangerous situation for that particular victim—revealing where she is or her activity—and put her very much at risk. It has to be instant and effective, and it has to be removed in perpetuity.

Q70 **Chair:** I apologise for pushing on this, but how quickly do you think instant should be?

Rachel Maclean: I do not know how to be clearer than that, Chair—as soon as it has been flagged.

Chair: Okay. Minister Philp, do you want to give us your thoughts on that?

Chris Philp: Ofcom will be obliged to publish codes of practice, which basically answers the question you have posed. For the benefit of the Committee, the duty to run these reporting and complaints processes are in clauses 17 and 18 of the Bill, but then there is an obligation in clause 37(10)(g) and (h), which requires Ofcom to publish codes of practice setting out what you have asked, so they are going to have to publish these before the Bill becomes effective.

Q71 **Chair:** You are the Minister; what are your thoughts on how clear, how accessible and how instant?

Chris Philp: In terms of the speed of action, it will be slightly context specific. If there is any live risk to someone, it should be instant. Removing images of someone that have been put up without their consent should take hours or a very small number of days. The idea that someone's image should be left up without their consent for any extended period is abhorrent. The condition around ease of access, including by children, and transparency means that the complaints form should be a single page, and there should be no more than a screen of text. You cannot have 20 pages of terms and conditions to wade through, or a form that requires you to go



HOUSE OF COMMONS

to six screens. It should be ultra-easy to use, including by children, as the Bill says on its face.

Q72 **Chair:** We have all probably had times in our lives where we have tried to complain about services via online forms. My most recent one was with Eurostar. Should it be literally a button on the front page of the website? Should it be that prescriptive? You have used the example of a child; I would use the example of somebody with learning difficulties.

Chris Philp: It is very important that the facility to report issues and make complaints cannot be buried three clicks away from the front page. It has to be prominent and easy to use. The details of that will obviously get set out by Ofcom in the codes of practice and is not for me as a Minister, but you have asked me to express my personal opinion, and, to the extent to which that is worth anything, a button that is always visible when you are browsing would be a good idea because you do not have to navigate away if it is just there the whole time.

Q73 **Chair:** Thank you for that. I do think it is imperative that account is taken of the needs of those users who might have additional challenges around using technology, learning difficulties, perhaps those do not have English as their first language, and who have problems with reading and writing. A whole raft of people might find an online complaints system difficult. It is important that Ofcom get that steer from this Committee and from the Minister.

Just a final question to both of you from me, and then I will bring in any other Committee members if they have any additional ones. We sometimes hear from the victims of sexual offences that they find it difficult to report offline offences. Is this Bill going to make it easier and more straightforward for them to be able to report offences online, and is it going to give them the confidence to do so? Rachel?

Rachel Maclean: Absolutely. That is the intent of the Bill and what we want to happen. That is why we brought the Bill in and have empowered Ofcom, giving them the resources, powers and legislation to do so. It is really important to acknowledge the truth of your statement—that victims of sexual violence have experienced difficulties in reporting.

All the work that I am doing in the Home Office alongside my colleagues in the MOJ—specifically Minister Atkins and the Lord Chancellor, around the rape review—is specifically designed to turn that around. We have committed to that. We want to improve the system. We are already making some changes. We know we have a long way to go, but I am sure you will have noticed the funding that took place in the latest spending review. I do not have the figure in front of me, but it is something like £300 million that we are spending to support victims of sexual violence across the board in the offline space, whether it is complaining to the police, getting that support in the court system, support through the ISVAs and IDVAs, or everything that we are doing with the police to improve their response when people first go to the police.



It is a very valid question. We want to improve the offline experience, but I am confident that this will bring the online sphere into a much better place for those victims.

Q74 Chair: Thank you. Minister Philp, when this Bill has been discussed and debated, we have often heard the challenge of future-proofing it. Earlier you said that this is not going to be revisited for the next five years or so. In those five years, all sorts of platforms will appear that we have not even dreamt of. Are you confident that it is future-proofed, and how?

Chris Philp: Yes, you make a very valid point. The Bill is constructed to be technology agnostic. Whether it is the duties being imposed on companies or the measures they can take to discharge their duties and keep people safe, we do not specify the technology at all. In a whole range of different areas, this technology moves on an almost monthly basis. To give you an example, when the Bill was drafted, the metaverse did not exist at all, but the metaverse is covered by this Bill because the definition of user-to-user services is constructed so that any user-to-user service regardless of technology—could be holograms or anything—is covered by the Bill. The metaverse was suddenly invented, effectively a few months ago, and it is covered.

To take another example, let us look at the age assurance stuff that we touched on half an hour or so ago. In the next few years there are going to be all kinds of age assurance technologies that we have not thought of today, or the ones that exist, like facial recognition and facial scanning, will become a lot better. That is why we do not specify on the face of the Bill what specific technology is or is not allowed. We specify the outcome. It is then up to the companies to deliver that, and Ofcom to make sure that they do. Obviously, they can update their codes of practice from time to time to stay up to date. The Bill is technology agnostic, which is the key thing.

Q75 Chair: Final question from me: you made a comment earlier about individual executives being personally criminally liable—that a named executive could find themselves in very deep trouble with the police if they obstructed information, lied, etc. How will the complainant, Ofcom or whoever be able to identify that named executive? We all know that when dealing with these enormous corporations, they are largely faceless. How are we going to find the named executive—or do we just fire all complaints at Nick Clegg?

Chris Philp: We all know where to find him!

Personal criminal liability, which carries a prison sentence of up to two years, relates to the obligation on these companies to provide Ofcom, as the regulator, with information. Each company has to nominate a named senior manager who is responsible for providing that information, and he or she is the person that is gone after if they do not provide it.



HOUSE OF COMMONS

There is an additional clause that I recall debating in Committee yesterday, which says that another senior executive, such as the chief executive or another senior board member, who does not necessarily have to be the named person—but somebody else who has overall management responsibility—can also be held responsible. I guess that is to avoid the company naming some very junior person to put them in the firing line.

Q76 Chair: If they have to provide to Ofcom this named executive, is there a danger that they will just be a permanently rotating selection of names, or are measures being put in place to prevent that from happening?

Chris Philp: That is why there is this additional provision—that, in addition to the named person X, there is also the possibility that another senior executive with general responsibility can be prosecuted as well, to avoid abuse of that named person provision. They could just find a very junior person and make them the fall guy, which is why the very senior executive can be brought into the scope of the personal liability as well, like the chief executive.

Chair: Okay, thank you for that. Does anybody have any additional questions? Kim.

Q77 Kim Johnson: Minister Philp, I just want to know what repercussions there should be for online platforms that fail to meet their duty of care. There have been some suggestions about sanctions and fines that could be used to support young people who have experienced harmful content online.

Chris Philp: In terms of the sanctions taken against companies, there is the criminal liability that I mentioned a second ago on individuals in relation to providing information to Ofcom. There are then the fines, of up to 10% of global revenue, which could run into billions, and as an extreme measure there is the denial of service and denial of access, where they are basically unplugged from the internet.

In terms of where the money goes, there are two sources of money that the Bill provides for. One is the fees that Ofcom can charge the industry to cover their own costs in discharging these duties in monitoring and regulating the industry—and, following a Government amendment this week, recouping their set-up costs as well. It is the “polluter pays” concept, where the industry will pay Ofcom the costs Ofcom incur. It will not be paid for by the general taxpayer—by your constituents or mine—but by the companies being regulated, which is really important.

Secondly, obviously our hope is that they comply, and do not get fined, but if the fines are levied, in common with other regulatory regimes, it goes into the general fund—the Treasury—and then, via spending reviews, gets allocated out. Clearly, if significant money in fines flows from social media firms to the Treasury as a result of this Bill, no doubt Rachel and her Ministry of Justice colleagues will be pointing to that in their negotiations with the Treasury when it comes to getting funding for victim services and so on.



HOUSE OF COMMONS

Rachel Maclean: We certainly will.

Q78 **Kim Johnson:** Thanks Minister, that sounds great on paper. I just wanted to know whether you believe that Ofcom have the powers and the resources to be able to implement everything that you have just said?

Chris Philp: They definitely have the powers and resources. The Government have funded them this year and next year, with £88 million of taxpayers' money and £20 million the year before that—£108 million in total—to get ready for this. That will then get recouped from the social media firms over the following three to five years. Thereafter, Ofcom will basically levy on Facebook and all the rest of them the fees and charges necessary to cover Ofcom's costs, and it will be the polluter that pays, not our constituents.

Q79 **Dame Caroline Dinanage:** Welcome, all of you. Earlier I asked Ofcom whether their approach was intended to be proactive or reactive when it comes to identifying and taking down inappropriate content, and they said both. But Chris and Orla, you have spoken much more about the proactive aspect of this. I am just a little bit concerned about the balance between the extent to which you regard Ofcom's role as actually going out there, tracking this stuff down, making sure that all the terms and conditions are being appropriately applied, and the extent to which you think their job is to sit back and wait for the complaints to come rolling in from their super-complainers or whatever else.

Chris Philp: As I said, I would expect Ofcom to do a combination of both. Clearly where there is a super-complaint, they are legally bound to respond to that as set out in this Bill. If they get significant numbers of complaints from members of the public individually, I would expect them to be responsive to that.

Like any good regulator, I would also expect them to be horizon scanning and actively thinking about where risks arise, and then dedicating their time and attention to particularly high areas of risk. For example, I want to prioritise anything to do with children's safety. There are some duties set out in clause 103 in the new version of the Bill, as opposed to the draft version, to do with making sure there is active scanning for terrorist and sexual exploitation content.

If I can just be upfront, one thing that worries me is that in Europe a couple of years ago, Facebook stopped scanning messages for child sexual exploitation and abuse images, citing data protection legislation as a concern. They have now thankfully reversed that, but a high number of child sexual exploitation images would have been missed as a result. I am worried about the impact that encryption might have on that, so I would expect Ofcom to be particularly attentive to that scanning point, because there are thousands of paedophiles who are identified via the scanning, and it is really important that that continues.



I would also expect Ofcom to pay particular attention to the platforms that either have the largest reach—like Facebook, because so many people are on it—or which have particularly risky functions, for example where there is evidence of paedophiles using particular services to identify children to groom, hence I would expect them to be proactive on a risk axis and on a scale axis.

Dame Caroline Dinenage: That is helpful, thank you.

Q80 Elliot Colburn: I would like to take you back to protected characteristics, if I may. Obviously, our inquiry is about pornography and its impact on violence against women and girls, but of course the online space can prove harmful for anyone, regardless of who they are. Just to bring up a few examples, we see racism happening online at huge levels. We see homophobia, biphobia, and particularly transphobia at the moment, happening online at very high levels. We see threats to out people, for example.

Are you confident that the Online Safety Bill and the codes of practices that we are expecting Ofcom to develop will give adequate attention to people's protected characteristics contained in the Equality Act, and therefore that there will be strategies in place to deal with these issues, particularly where intersectionality comes in, which can prove infinitely more complex? How confident are you that the Bill and the codes of practice that will come after it will take account of that?

Chris Philp: Thanks for the question, Elliot; I am confident. The first point I would make is we already discussed how, at the very start of this Bill, in those two clauses I referenced, the risk assessments have to account for characteristics. As you will know, under the Interpretation Act 1978, the singular is taken also to mean the plural, so it will also have to consider those intersectional points where a particular individual has multiple characteristics—like being gay and ethnic minority—and where those things come together to create additional risk. That is covered and considered.

Secondly, in due course by statutory instrument we are going to be specifying the matters covered for content that is legal but potentially harmful, which is an opportunity to consider some of these issues and make sure they are specifically covered.

The third point I would make is at clause 150, we are introducing a new harmful communications offence to update the old the Malicious Communications Act 1988, which will cover some of the things you are pointing to.

Q81 Elliot Colburn: I appreciate you have been grappling with this in Committee and it has been a big point about the Bill, and I have no wish to revisit all the arguments around legal versus harmful and the differences between them, but can I just ask that you take away some of these particular concerns—particularly the concept of outing someone, for



HOUSE OF COMMONS

example? That is technically legal, but it is certainly harmful, so could I just ask you to take that away as you are developing those further bits?

Chris Philp: Yes, we definitely will do that as we are developing the list that I just mentioned. It is also worth considering the point you made about outing in the context of the new harmful communications offence, because if someone intends to cause harm, and in the message they send there is a real and substantial risk that it would cause harm, the definition of harm here is “psychological harm amounting to at least serious distress”. I am not a lawyer, so I do not want to make a definitive statement, but it is possible that what you have described, Elliot, would contravene the harmful communications offence being created in clause 150.

Elliot Colburn: Thank you, Ministers. Thank you, Chair

Chair: Thank you. I think that is it for questions from the Committee. I thank both Ministers and your officials for attending this afternoon, and draw the meeting to a close.