HOUSE OF COMMONS

Home Affairs Committee

Oral evidence: Home Office preparedness for Covid-19 (Coronavirus), HC 232

Wednesday 13 May 2020

Ordered by the House of Commons to be published on 13 May 2020.

Watch the meeting

Home Affairs Committee Members present: Yvette Cooper (Chair); Ms Diane Abbott; Dehenna Davison; Ruth Edwards; Simon Fell; Andrew Gwynne; Dame Diana Johnson; Tim Loughton; Stuart C. McDonald.

Digital, Culture, Media and Sport Committee Member present: Julian Knight, Chair.

Questions 507-587

Witnesses

I: Caroline Dinenage MP, Minister for Digital and Culture, Department for Digital, Culture, Media and Sport, and Baroness Williams of Trafford, Lords Minister, Home Office.

Examination of witnesses

Witnesses: Caroline Dinenage MP and Baroness Williams of Trafford.

Q507 **Chair:** Welcome to this online evidence session for the Home Affairs Committee. This is part of our ongoing work on the response to the coronavirus crisis, but looking more widely at online harms, crime and abuse. We are grateful to the Ministers—Caroline Dinenage from DCMS and Baroness Williams from the Home Office—for joining us to give evidence today. I welcome the Ministers—thank you very much for your time. Julian Knight, Chair of the DCMS Committee is also with us.

We want to cover a wide range of issues around what is happening online in the coronavirus crisis, as well as the Government's response and the Online Harms White Paper. Baroness Williams, to start, could you give a very short answer on what most worries you at the moment in terms of the things that you have seen happening online during the coronavirus crisis?

Baroness Williams: Thank you very much for inviting me to join the Committee this morning. There are probably three things that worried me most in the run-up to the lockdown period. The first was CSEA online, because of course, 98% of children are not at school. The second thing that worried me was domestic violence and harms related to that. The third thing was online extremism or, indeed, physical extremism. Those are the things that exercised me most in the run-up to the lockdown period and, I suppose, on which I have been keeping the closest eye throughout the period.

Q508 **Chair:** What has troubled you most in what you have seen happening over the last few weeks?

Baroness Williams: I expected to see more reports from the police on domestic violence. The fact that there have not been as many as I would have expected worries me, but we have yet to see what will happen coming out of lockdown. On extremism, we have not seen an uptick generally, but during the lockdown period—having spoken to Mark Hamilton, who, as you know, is our lead on hate crime—there has been a 21% uptick in hate incidents against the IC4 and IC5 communities.

You will obviously have seen the stuff on 5G masts. Some of that is harmless conspiracy theorist stuff, but other elements are more serious when people attack what they think are 5G masts. They are actually attacking 3G and 2G masts as well, because some of them cannot tell the difference.

On CSEA, we are just so alert to what might be happening online. We have put a lot of funding into keeping children safe and helping adults to spot some of the signs at home when their children are online. The DFE

announced that the Government will make funding of £1.6 million available to the NSPCC to help adults who are worried—

Chair: I will come back to that as we want to pursue it in more detail shortly.

Baroness Williams: I will keep it high level—those are the three things. Finally, on domestic abuse, we are seeing a real uptick in calls to helplines.

Chair: Thank you. Caroline Dinenage?

Caroline Dinenage: Good morning, Madam Chairman and the Committee—thank you for having me. We know that, as anticipated, more people, particularly children, are going online during this crisis. Of course that presents lots of benefits, but also some dangers and some risks. It is too early to be able to confidently analyse any real patterns, but I had a roundtable meeting, alongside the Security Minister, a couple of weeks ago with some of the child safety organisations, and anecdotal evidence suggests that about 60% of calls that some charities are receiving are related to children's mental health safety issues as they are cut off from friends and schoolmates during this period. Parents also have concerns about how they keep their children safe online. Often they would approach teachers and trusted people in the school to tackle some of these issues, and of course that path is not always open to them at the moment.

Another concern, as Baroness Williams has already articulated, is about misinformation and disinformation. Clearly, accurate information is really important at the moment—more important than ever. Misleading information about covid-19, whether it is maliciously intended or not, could actually or potentially risk lives, which is why that is of concern to us.

As for adult users, we have seen an increase, a concerning increasing trend, in things like revenge porn and sexploitation, and calls to helplines along the lines of things like that, over this period.

The other thing I would like to mention is online fraud. Although the number of cases reported to Action Fraud is actually lower than usual, there is some covid-related fraud out there. About 1,300 covid-related frauds and cyber-crimes have been reported, so that is something to be mindful of as well.

Q509 **Ruth Edwards:** I should start by drawing attention to my entry in the Register of Members' Financial Interests and particularly my recent employment, until the election, with BT's cyber-security team.

Ministers, thank you very much for joining us. I want to start by going back to the issue of 5G conspiracy theories. As you mentioned, Baroness Williams, we have seen vandalism against the physical infrastructure of the network itself in the last couple of weeks, but also many assaults on telecoms engineers. One engineer, I understand, has been stabbed; others have been spat at and screamed at in the streets. What is the

Government doing to tackle the dangerous and often criminal consequences of this disinformation campaign?

Baroness Williams: I think you could probably categorise the disinformation into two elements. There is that which is harmless conspiracy theories and that which actually leads to attacks on engineers, as you have said, but there is a far-right element to this as well. Therefore, when a criminal offence is committed, clearly it's a serious thing. The police, I know, have been monitoring this. I go on the operational calls with the Home Secretary every single day. I know they are very alive to it and monitoring it, and they are dealing with it.

Ruth Edwards: Minister Dinenage?

Caroline Dinenage: Ruth, as you know, the vast majority of misinformation and disinformation is harmful but legal. In the case of some of the crazy misinformation about the safety of 5G masts, it is in many cases inciting criminal damage, which is an illegal offence, and that is why we are working very closely with the Home Office on it.

In terms of what we have been doing to help tackle it, very early on in this crisis we set up the cross-Whitehall disinformation unit. As the name suggests, it goes across Government, but it also includes academia, the military and some of the companies involved. It looks at a number of threats and then passes the worrying concerns on to the companies and requests that, if it is against their standards and their regulations, it be taken down. So we are working very closely with them to really tackle this disinformation and misinformation at source. For example, we were working with Twitter, so that when anybody went online on Twitter and searched "covid-19" in relation to 5G masts, it would direct them to the correct information on the Government website.

Q510 **Ruth Edwards:** I know that industry and Government have been doing quite a bit, but do you think that is proving enough—do you think it is being effective? I understand that a recent Focaldata poll showed that 27% of the public said they could not rule out a link between 5G and coronavirus, 8% believed there is a link, and 19% are unsure. So over half the respondents either believe that there is a link between coronavirus and 5G or they are not sure and feel they cannot rule it out. To me, that is pretty serious, given how our economic recovery is going to rely on things like the safe roll-out of 5G. I appreciate that there are some elements, such as far-right elements, who are stirring this up for even more sinister reasons, but I do not think that any element of the conspiracy theory can be categorised as "harmless", because it is threatening public confidence in the 5G roll-out.

Caroline Dinenage: From my perspective, I think you are right. That is why I said from the beginning that accurate information is more important now than ever, because lives are literally at risk, even if misinformation is spread unknowingly or completely without malicious intentions.

At the beginning of the covid period, we also saw that there was a fake nurse online, spreading completely erroneous coronavirus cures.

Technically, there is nothing illegal about that. It is very disingenuous, but at a time when we are not only worrying about people's physical health but their mental health, content like that can be really harmful. And that is why we have been working closer than ever with the platforms to make sure that misinformation like that is addressed as quickly as possible and taken down, but more broadly so that people are directed to the correct information. So Facebook has recently started contacting people who have engaged with content that has subsequently been taken down and directing them to the correct information.

Q511 **Ruth Edwards:** That is great to hear. Thank you. My final question is: are you concerned that it might lead to a delay in the roll-out 5G if these sorts of attacks, both on the network infrastructure and on engineers installing it, continue?

Caroline Dinenage: We are working very closely with my colleague Matt Warman in the Department for Digital, Culture, Media and Sport, who is working really closely with the companies that are rolling 5G out. Clearly, it has been worrying and it is not in any way an ideal situation. Let's face it—these masts are telecommunications infrastructure, and as you have heard from Baroness Williams, there has been a fairly random scattergun approach as to which bits of that infrastructure have been attacked. They are crucial, for enabling people to continue to work and for our emergency services to continue to operate. So there is a whole lot of impact here, but, no, I do not think it has had any meaningful impact on the roll-out.

Ruth Edwards: Thank you. No further questions, Chair.

Q512 **Dehenna Davison:** Thank you to both Ministers for being with us today. My questions are again on the disinformation point. I think it is incredibly troubling seeing some of the figures, such as Ofcom finding that in the first week of lockdown around half of everyone had encountered misleading or false information, and two thirds of those said they had seen it at least once a day. But we know that a lot of the misinformation is actually based around correct information that has been slightly reconfigured or twisted. What is your response to that? How do you think that that can be tackled? I will go to Minister Dinenage first.

Caroline Dinenage: It is very tricky, isn't it, because where content is harmful but legal, or misleading but legal, we also have to consider people's rights to freedom of speech. The difficulty has been compounded by the fact that during the covid-19 process, sometimes misinformation can be damaging to people's health and wellbeing, as we have heard.

That is why we have been working very closely with the social media platforms; that is why we have got this cross-Government disinformation cell that has sprung up. We have only used it twice before—once in the EU elections and once in the general election just before Christmas—so it's quite a new concept. It's all about trying to predict where those pieces of misinformation and disinformation are coming from, trying to stem them upstream, and making sure that the platforms are aware of them so that they can take aversive action where possible. Clearly, it all has to be done

within the realms of protecting people's freedom of expression and freedom of speech, and in many cases there is nothing technically illegal about what they are doing. In many cases it does not actually contradict some of the platforms' standards or regulations.

Q513 **Dehenna Davison:** Is that a concern for you? Do you think that social media companies should perhaps look into those regulations to try and tackle this a little bit more strongly?

Caroline Dinenage: This is one thing we are looking at as part of the online harms work: how you protect people's right to freedom of speech and freedom of expression, and, alongside that, how you also protect people who are online from harmful and exploitative information that could damage them. These are all questions that we wrestle with, because it is quite a difficult balance to strike. A lot of this is about companies having the right regulations and standards and duty of care, and that will also be in the online harms Bill and online harms work. If we can have more transparency as to what platforms regard as acceptable—there will be a regulator that will help guide them in that process—I think we will have a much better opportunity to tackle those things head-on.

Q514 **Dehenna Davison:** Thank you. Baroness Williams, what are your thoughts?

Baroness Williams: I agree with Minister Dinenage's point that there is a balance to be struck between freedom of speech and removing and dealing with stuff that is harmful to people. You asked me at the beginning what my worries were. People attacking 5G masts was not in the list of top five things that I was worried about. All sorts of unexpected things have come out of this. One thing we are all probably agreed on is that through this crisis we all—all aspects of society—have to pull together, and it is not helped by figures in mainstream media promoting that there might be some truth in it. We have all got a responsibility, but I fully uphold people's right to free speech.

Q515 **Dehenna Davison:** I have one final question. As it stands at the moment, do you think that social media companies are doing enough to tackle false information?

Baroness Williams: Caroline went through the counter-disinformation cell and some of the things happening online. The thing about the online world is that quite often it is reactive. Unless it is illegal, it is very difficult to make it proactive.

Q516 **Dehenna Davison:** Minister Dinenage, do you have thoughts on that?

Caroline Dinenage: I do have some thoughts on that. We have seen how some major platforms have updated their services and standards as a direct result of covid. We have also seen some really good proactive work. I have already spoken about Twitter and Facebook and some of the things they are doing. WhatsApp have changed the ability to be able to forward information to a big chunk of people—you may have seen that. YouTube have enabled us to roll banners directing people to NHS information. There has been some really proactive stuff going on. We have never really seen

the like of that before, but it now shows that it is possible for platforms to work at great speed and with great integrity to address some of these concerns. I would like to see a lot more of that as we move out of the covid period to deal with other concerns and other harms that we are worried about.

Q517 **Julian Knight:** Just coming in on that final question from Dehenna Davison—this is for Minister Dinenage—the latest figures from Ofcom show that 47% of the public have seen disinformation concerning covid-19 in the past week alone. Also, I have just got an email from Rebecca Stimson, the public policy manager at Facebook, that says that the programme that you have discussed in terms of redirecting users to proper, correct information is not up and running yet; it is just a press release at the moment. In the light of that, do you still think that these companies are, as you said to the Lords yesterday, excellent in addressing the concerns that you have raised on this issue?

Caroline Dinenage: I think I should clarify what I said to the Lords yesterday. Some of them have been excellent. There is still an enormous amount of progress to be made. The Secretary of State made it clear, when he had a meeting with some of the major platforms quite recently, that there is still a long way to go and that we expect more.

With regard to the number of people who see disinformation and misinformation, there is another aspect to that, which is about how we make sure people have digital media literacy. That was a commitment in the Online Harms White Paper. It is a piece of work that we will be rolling out and announcing more about later in the year. At the moment, we are doing an audit as to what is already available.

To give you an idea about what I am talking about, Ofcom published a report on people's attitudes to digital media and found that over half of internet users—about 54%—say that they consider only some of the factual information they find online to be true. We want to get to the position where not only do we have the ability to make sure that can remove harms online, but the people consuming online content have the resilience, and the technical and discerning know-how—the digital media literacy—to be able to question facts and not take everything as read.

Q518 **Julian Knight:** Minister Dinenage, given that you effectively just said that more needs to be done by social media companies, in terms of tackling disinformation in double-quick time, do social media companies have a problem with democratic scrutiny? As you saw in front of my own Committee just the other week, they would not answer the most basic questions concerning this. Also, Mark Zuckerberg has been in contempt of Parliament. Do you think they have a difficulty with democratic scrutiny? How does this inform your approach to regulation? Can they be trusted?

Caroline Dinenage: I do not have enough evidence to be able to make a decision as to whether they have an issue with democratic scrutiny, but I think—

Q519 **Julian Knight:** Sorry, they are in contempt of Parliament. Mark

Zuckerberg is in contempt of Parliament. Last week we had them in front of us and endured an hour of them not being able to answer questions, frankly. If they can't do that, how will they respect a regulator?

Caroline Dinenage: I am not here today to defend big tech companies—that's the last thing I want to do. My job is a difficult balance between creating an environment where tech companies can grow—we are the tech capital of Europe and tech companies are growing at six times the rate of the rest of the economy—and having responsibilities to freedom of speech, to allowing the sector to work in as free and easy a way as possible, and to protecting vulnerable people online. I never want to look into the eyes of a family and say I wasn't doing everything I could to protect vulnerable people.

We need to acknowledge that this work is not just happening here. The eyes of the world are upon us and the online harms work that we are doing is world leading. That is not to say that everyone else isn't looking at what we are doing with a view to doing more of the same. Other countries have put in place some changes, but they have been piecemeal.

Our work is the most comprehensive system of changes and will bring about some quite radical reforms to the way we do things. Companies have to face up to that, because it is coming down the track. It won't just be here that it happens. Around the world, countries are looking at how we are implementing this. The companies need to engage with democracy and with the regulations that are coming.

Q520 **Julian Knight:** Talking about coming down the track, the Secretary of State has eulogised about the UK being a centre of data. Is the price of that ensuring that the legislative architecture for social media is light touch? Does that explain why there has been a widely reported rowing back on the timescale and scope of online harms legislation?

Caroline Dinenage: As I have said, this is not easy. This is never going to be an easy balance to strike. We want to make the UK the safest place in the world to be online; we have said that publicly on a number of occasions. However, we have also said we want the UK to be the best place in the world to start and grow a tech company. We rely on big tech industry in our economy; in 2018, it contributed £149 billion to our economy.

The two are not mutually exclusive. If we can build consumer trust and transparency in the online platforms, that is only going to be adding power to their elbow in terms of their ability to be able to communicate with people. People need to be able to trust them. There is no rowing back on the Online Harms White Paper—let me just tell you that for a start—and there is no massive delay to it either. Clearly, there have been some slight impediments, in that the covid-19 crisis has eaten up some of the parliamentary time that would otherwise have been available, but the Home Office and the Department for Digital, Culture, Media and Sport are working as hard on this as we ever have.

In fact, although covid-19 has provided some obstacles, it has been an interesting test case for what some of the threats are, and how significant things like misinformation and disinformation can be, with the 5G masts and other examples. Taking some of the learning from covid-19 has been really useful as we prepare the two things we are working on: our full response to the White Paper consultation and the legislation that will go alongside it.

Q521 **Julian Knight:** I have two final questions for you. On the regulatory architecture, what has prevented the Department from taking the final decision on the regulator? How will you ensure that the regulator is properly resourced and, crucially, has the skills to do the job?

Caroline Dinenage: We set out in our interim response to the White Paper that we were minded to appoint Ofcom. The reason we made that decision is that it has the experience and capacity—the scale, if you like—to take on an enormous role like this, although it may not necessarily have the technological expertise at the moment.

When we put out our full response, it will confirm which company we are minded to appoint, and then of course that will go through the legislation. That will give it time to make sure it is working up to having the necessary expertise. It is about having an organisation that is already robust and working at a very high level, with an enormous amount of content.

On funding, we have said publicly that initially it will be Government-funded, but then we are working towards a situation where there is no taxpayer funding for the regulator; it will be funded from business.

Q522 **Julian Knight:** This is my final question. Last year, the Digital, Culture, Media and Sport Committee, in its report on immersive tech, called for lootboxes in games to be strictly controlled. Do we have to wait for a review of the Gambling Act to see action on this area of online harm, particularly for young people, or will you take action now through section 6 of the Gambling Act?

Caroline Dinenage: We do take concerns about lootboxes in video games really seriously, which is why we have committed to a review of the Gambling Act, with a particular focus on that. The DCMS Select Committee has also done an inquiry on immersive and addictive technology, which we have welcomed, and has brought up some really important and complex issues. We will be responding to that soon.

There are other things ongoing at the moment. We have been doing some work with PEGI, which is administered by the Video Standards Council, on content descriptor labels. We are working alongside UKIE, the video game trade association, with its "Get Smart about PLAY" campaign to make sure more parents are using the parental filters, which allows them to take active control over children's gaming and their ability to purchase lootboxes.

In August, Sony Interactive Entertainment, Microsoft and Nintendo announced that all future titles on PlayStation, Xbox and Switch will be

required to disclose the relative probability of receiving randomised virtual lootboxes. That is going to be implemented this year. There is a whole range of schemes going on alongside Government legislation and inquiries to look at that concerning issue.

Chair: Thank you very much. Excuse my temporary absence; I had a few technology hitches.

Q523 **Andrew Gwynne:** Before I ask a question, I want to add to my declaration of Members' interests the fact that my wife is an executive member for neighbourhood services at Tameside Metropolitan Borough Council, which includes community safety. In that role, she is a member of the Greater Manchester Combined Authority police and crime panel.

Minister Williams, in respect of the disinformation that we know is online—and we have seen examples of this—a number of these conspiracy theories have been jumped on by the far right, and particularly far-right groups in the UK and across the EU. Indeed, a report by the Zinc Network, a communications agency that tracks disinformation and propaganda, claimed that these groups are trying to "utilise the pandemic to bring new relevancy, attention and support for their key grievances" and that they have uncovered far-right groups in the UK "using Covid-19 to promote a British form of fascism". What is the Government doing to combat this?

Baroness Williams: Andrew, I can concur with you that this sort of stuff is happening online. Extremists will use any occasion to exploit their narrative and to spread false information and conspiracy theories to, obviously, promote their own agendas and to divide communities.

We have observed extreme right-wing narratives falsely link the spread of covid with a number of issues, including immigration, racist accusations that some parts of the community are not complying with the lockdown or, indeed, are inferior. In addition to rebutting the disinformation where we see it, we have engaged with CSPs to ensure that they respond as effectively as possible. Our work to raise awareness of disinformation online through the "Don't Feed the Beast" campaign, the Home Office work across Prevent and counter-extremism, CCE, is playing a key role in countering these covid-19-linked extremist narratives and, we hope, safeguarding our communities.

Q524 **Andrew Gwynne:** Thanks for that. Of course, some of the examples that we have seen are really pushing against that sense of injustice and grievance—the usual scapegoating, often, of minorities, as you say. Certainly we have seen some pretty vile anti-Jewish conspiracy theories, blaming Jews and Israel for creating the virus. Are you working with organisations like the Community Security Trust to ensure that there is community cohesion within not just the Jewish community but the wider community across the UK?

Baroness Williams: Absolutely, Andrew. The Jewish community; Tell MAMA, who do the anti-Muslim monitoring—of hate crime; the Chinese community: I know that, when I was speaking to ACC Mark Hamilton

yesterday, we engaged very early with them, and that's absolutely crucial as an example of working together to not only provide reassurance but to tackle some of the activity where it exists.

Q525 **Andrew Gwynne:** Can I bring in Minister Dinenage, please? Minister Williams has mentioned the "Don't Feed the Beast" campaign, but I just wondered how, specifically, with the information that we have seen, there is targeted work going on, and liaison with the social media platforms, not just to fact check some of this disinformation, but—the most vile—to take it down.

Caroline Dinenage: Yes, this is part of our ongoing work, and this is why we have stood up this cross-Whitehall covid group, to be able to do this more quickly and more comprehensively, working with the Cabinet Office, who do a lot of the comms around this. They are working closely with some of the military operators, including 77th Brigade.

With regard to our role in DCMS, it is more as a co-ordinator bringing together the work of all the different Government Departments and then liaising directly with the platforms to make sure that their standards, their regulations, are reflective of some of the concerns that we have—make sure, in some cases, that harmful content can be anticipated and therefore prevented, and, where that is not possible, where it can be stopped and removed as quickly as possible.

Q526 **Andrew Gwynne:** And are you experiencing any difficulties with some social media platforms in tackling some of these issues?

Caroline Dinenage: We have found that we have become—I forget the proper term, but we have become like a trusted flagger with a number of the online hosting companies, with the platforms. So when we flag information, they do not have to double-check the concerns we have. Clearly, unless something is illegal, we cannot tell organisations to take it down; they have to make their own decision based on their own consciences, standards and requirements. But clearly we are building up a very strong, trusted relationship with them to ensure that when we flag things, they take it seriously.

Q527 **Andrew Gwynne:** On that trusted relationship, is there any commonality across the various platforms in terms of fact-checking some of this disinformation?

Caroline Dinenage: I do not have that information to hand at the moment, but I am happy to have a look at that and drop you a note if there are any discrepancies in the way they are responding.

Baroness Williams: I just want to make a very brief point. There is obviously that which is illegal and that which breaches the CSPs' terms of use. It is that latter element, particularly in the area of extremism, on which we have really tried to engage with CSPs to get them to be more proactive.

Q528 **Ms Abbott:** I thank both Ministers for giving evidence before the Committee. Both Ministers have kept referring to freedom of speech,

which is very much the mantra of the big tech companies: Facebook, Twitter and so on. They are US-based tech companies who are very conscious of what they would describe as their first amendment rights. What do you say to people who argue that a willingness by Government to defer to big US tech companies has constrained its ability to move against online harms?

Caroline Dinenage: As I said, the whole issue around online harms will always be finely balanced. That is why we have the online harms legislation coming down the track, which will make things a lot clearer for companies and users—and there will be a regulator.

On the one hand, as I said, we want the UK to be the safest place in the world to go online. We also want to be able to encourage tech companies, which are so important for our economy—before the covid crisis started, they were growing six times faster than the rest of the economy—and really important employers.

At the same time, it is vital that we protect the safety and security of our citizens going online. Meanwhile, we do have a thriving democracy in our country, which is one of our cornerstones. It is a country where pluralism and freedom of expression has always been protected. It is not an Americanism; it is just a fact that we always need to balance those sometimes conflicting challenges in order to bring forward some sort of legislation that will establish a new duty of care on platforms, that will improve internet safety for everybody and that will be overseen by an independent regulator that will have the best interests of our citizens at its heart.

We believe this could be world leading and lead to a brand-new global approach to online safety that supports our democratic values and promotes a free, open and secure internet.

Q529 **Ms Abbott:** I believe in parliamentary democracy—I've been an MP for 32 years and would not have been doing it for 32 years if I did not believe in the democratic process—but some people, like me, would argue that there is a difference between freedom of speech exercised in your own name, at a public meeting, with someone coming up to you in the street or writing you a letter, and freedom of speech exercised in anonymity.

In 32 years in politics I have seen that there has always been abuse, but the ability to abuse people anonymously, using these online platforms, has increased the volume of abuse a hundred-fold. Do you accept that it is one thing to exercise your freedom of speech publicly, in your own name, but it is another thing to exercise your freedom of speech on an anonymous online platform?

Caroline Dinenage: Yes, absolutely, Diane. You have hit the nail on the head and I completely bow to your many years of parliamentary democracy experience. Online abuse is totally unacceptable and far too prevalent. Ofcom data says that close to half of UK adults say that they have seen harmful content in the last year. Not only that, this kind of faceless attack can bully people away from engaging in social media and

other platforms in which they might want to participate, so it is anti-democratic in many senses, as you have articulated.

There are a couple of things here. Alongside the online harms work that we are doing, we have also asked the Law Commission to review our laws on abusive and offensive online communication. They are going to be coming back with some recommendations, probably early next year. We are looking very carefully at their work as we are putting together the online harms legislation because we do not want to have a surprise—we want to be able to look at what they are likely to recommend.

The other thing I would say is that we have to be really careful as we have to be able to protect people's right to anonymity in some cases. In some parts of the world, as you know, people do not have the same freedom of expression and freedom of rights, the opportunity to whistleblow or the opportunity for journalistic expression. Sometimes people are victims and feel that they have to act anonymously, because otherwise they could be in danger. We have to be really careful about saying that anonymous content is always bad, but you are absolutely right that in many cases it can be harmful.

Baroness Williams will talk more about this, but the police do have legal powers to identify individuals who attempt to use anonymity to escape any form of sanctions for online abuse, where their activity is illegal, and we are making it easier for the public to report online crimes in cases like that.

Q530 **Ms Abbott:** Finally, would you consider changing the regulation, so you could post anonymously on a website or Twitter or Facebook, but the online platform would have your name and address? In my experience, when you try to pursue online abuse, you hit a brick wall because the abuser is not just anonymous when they post, the online platform doesn't have a name and address either.

Caroline Dinenage: That is a really interesting idea. It is definitely something that we have been discussing. With regard to the online harms legislation that we are putting together at the moment, we have said very clearly that companies need to be much more transparent. They need to set out standards and they need to clarify what their duty of care is and to have a robust complaints procedure that people can use and can trust in. That is why we are also appointing a regulator that will set out what good looks like and will have expectations but also powers to be able to demand data and information and to be able to impose sanctions on those that they do not feel are abiding by them.

Q531 **Chair:** What does that actually mean? Does that mean that you think that the regulator should have the power to say that social media companies should not allow people to be anonymous?

Caroline Dinenage: As I have already said, I think we need to be really careful about anonymity altogether, because there are cases where people—

Q532 **Chair:** Anonymous to the platform; I don't mean anonymous to the public. Anonymous to the platform.

Caroline Dinenage: This is something that we are considering at the moment. There are a number of things here. In the online harms legislation, the regulator will set out their expectations.

Chair: We can't devolve everything to the regulator. Something like this is really important—should social media companies be allowed to not know who it is that is using their platforms? That feels like a big question that Parliament should take a view on, not something we just hand over to a regulator and say, "Okay, whatever you think," later on.

Caroline Dinenage: Yes, exactly. That is why we are considering it at the moment, as part of the online harms legislation, and that, of course, will come before Parliament.

Q533 **Chair:** Can I clarify when that online harms legislation will come? It had previously been said that it was going to appear in this parliamentary Session. Will it be coming in this parliamentary Session?

Caroline Dinenage: The choreography of this is that we have to do our full response to the White Paper. We did an interim response that was published in February. Our full response will be coming later on this year—quite shortly. At the same time, we will be working up the legislation and that is, obviously, out of my hands in terms of when the parliamentary slot for it will be, but we will be pushing for it as soon as possible. It is such an urgent piece of legislation for us. Both the DCMS and the Home Office are really keen to accelerate it as much as we can.

Chair: I will bring Julian Knight back in on that issue.

Q534 **Julian Knight:** Minister, I am a bit confused by that answer, because the Secretary of State said to our Select Committee that it would be coming forward in this Session. Matt Warman also said in February that it would be coming forward in this Session. Not much time has elapsed since then. Are you saying that it is not going to happen in this Session?

Caroline Dinenage: No, that is not what I am saying at all. What I am saying is that the full response will be later on this year, probably in the autumn, and then the legislation will follow in quite short order from that.

Julian Knight: In this Session, Minister?

Caroline Dinenage: Of course, our ambition is for it to happen in this Session.

Q535 **Julian Knight:** With the pre-legislative scrutiny that has been promised?

Caroline Dinenage: You will understand that since February, covid-19 has unravelled, and we have lost quite a large chunk of parliamentary time. We will be asking for a legislative slot, but it will be up to—

Q536 **Julian Knight:** Forgive me, Minister, but the Secretary of State appeared before us only three weeks ago, and he stated it would be in this Session

with pre-legislative scrutiny in this Session. Is that still the case?

Caroline Dinenage: That is still the very clear aspiration, yes.

Julian Knight: So it is an aspiration, not a commitment.

Caroline Dinenage: It is an intention.

Julian Knight: An intention? Thank you.

Q537 **Dame Diana Johnson:** Minister Dinenage, I want to follow up on the issue you raised about the Law Commission doing a piece of work that would feed into the online harms legislation. To follow up on what Julian Knight was just saying, you said that the Law Commission was doing that piece of work and it would be available next year. Is it the intention for any recommendations from the Law Commission to be part of any legislation that you want to bring forward?

Caroline Dinenage: The Law Commission work is quite a long piece of work. It has been going on for a while now and is not due to conclude fully until 2021. There may be new legislation that comes out as a result of that at the end. Clearly, we are working with them throughout the online harms Bill being brought together. We are picking their brains as we go along, because it is very important that any learning that they have already made from their investigation is included in our thinking.

Q538 **Chair:** May I come back to the issue about what it is that you are actually proposing and what difference it makes in practice, and bring in Baroness Williams on that? If harm is happening at the moment—whether it is covid conspiracies being spread or something illegal, such as some far-right escalation or the organisation of violence, the organisation of an attack on a 5G site, a hate crime or an incitement to racism or violence—in a closed Facebook group, are Facebook doing anything about that?

Baroness Williams: I am glad that you have asked that question. I am going to come in on the point of CSA here: last year, Facebook identified and removed 12 million pieces of CSA material from Messenger. They then announced that they were going to end-to-end encrypt Messenger. That, for us, is gravely worrying, because nobody will be able to see into Messenger. I know there is going to be a Five Eyes engagement next week, and I do not know if the Committee knows, but the Five Eyes wrote to Mark Zuckerberg last year, so worried were we about this development.

Q539 **Chair:** The encryption is an added problem, and we will come back to that. Another problem is their closed Facebook groups, some of which may have thousands and thousands of people in them and may include incitement to various crimes—we have seen examples of that. Are they still continuing to do nothing about Facebook closed groups and crimes that may be happening within those groups, and what are you doing about that?

Baroness Williams: I cannot really comment on the groups, but what I can say is that the takedown rates have hugely improved, if you are talking about Facebook in particular. It is important that law enforcement,

the regulator and Government are joined in expectation that these things will be removed and, where stuff is criminal, criminals will be brought to justice.

Q540 **Chair:** That is fine, but I cannot see it if it is in a closed group that I am not part of, so I cannot report it to the police. I am interested in these big Facebook groups in which we have seen examples of incitement to racial hatred, various violent crimes and so on. You have both raised concerns about the escalation of some of these problems during the coronavirus crisis, so I am interested in whether you have had any discussions with Facebook about what they are doing about their closed groups and, if so, what is happening.

Baroness Williams: I have not had discussion with Facebook on closed groups. The reason I brought up end-to-end encryption is that nobody can see into that, whereas both Facebook and law enforcement would have access to stuff that was not end-to-end encrypted.

Q541 **Chair:** Okay. Law enforcement do not have access to anything if they do not know there is a crime to be investigated in the first place. Minister Dinenage, have you had any engagement with Facebook on closed groups and what is happening, either during the coronavirus crisis or before?

Caroline Dinenage: This is something we are working on, and not only within the Department. We are working very closely with the Home Office on this. As Baroness Williams said, at the moment, the situation is easier because Facebook can in some ways police some of these closed groups, but if the end-to-end encryption comes in, that is of enormous concern for all of us. Officials from my Department and James Brokenshire, the Security Minister, met with the organisation quite recently.

Q542 **Chair:** Sorry, can I just interrupt you? I appreciate that the Messenger issue is a really important one, but I am asking a different question. I am asking about the closed groups where Facebook can in theory see what is going on—Facebook allows these groups to happen in the first place. Law enforcement cannot look into them unless some concerns have been raised with them in the first place, yet there is evidence that these big Facebook groups are used to incite hatred and violence, and, I have no doubt, also to spread all kinds of dangerous misinformation. We have previously raised this issue with Facebook, but they are clearly doing nothing about it at all; they keep saying, "We will come back to you", but then do not do anything. Are you aware that they are doing anything now, and have you raised this with them?

Caroline Dinenage: This is something you are absolutely right to raise; it is very important, and something we are concerned about. Facebook will say that they are working very closely with the National Crime Agency and—with regard to child protection, for example—with the US National Centre for Missing and Exploited Children, which is their contact there. They will say that reports from Facebook have resorted in more than 2,500 arrests by UK law enforcement on child protection—

Q543 **Chair:** Okay, but I think you are still answering a different question. I am specifically interested in these closed groups, where people cannot complain, which go broader than the child abuse issue where they have specific arrangements for identifying material. Put that aside. I am asking about things such as far-right organising, hate crimes and misinformation happening in closed groups. Are Facebook themselves now policing those groups?

Caroline Dinenage: I believe that they are. I might have to come back to you with a more detailed explanation of that. Susan might have more as well. The one thing I would say—if it helps in any way—is that we have made it very clear in the Online Harms White Paper that private channels will be within the scope of the regulation. But, obviously, we will have to take into consideration the greater expectation of privacy for users and freedom of expression—that awful balance with what is legal but harmful.

Q544 **Chair:** If you have 3,000 people on a closed Facebook group—or even several hundred people—who are organising or inciting crimes, that seems to me to be a significant issue that Facebook should be taking some responsibility for and that law enforcement should have a role in. Baroness Williams, do you want to come in on that point?

Baroness Williams: It might be helpful to the Committee to know that Facebook reported in its community standards enforcement report, released this week, that in quarter 1 of this year they have removed 4.7 million posts connected to known hate organisations compared with 1.9 million in quarter 4 of 2019. To me, that shows a bit of progress. But I cannot answer whether that was on a closed group. They deleted 9.6 million posts containing hate speech, compared with 5.7 million in quarter 4 of 2019. They put warning labels on 50 million pieces of content related to covid-19. I know that tools for directing terrorism work across the platform include those closed groups.

May I add something else? It might be taken up next week. I know that the Home Secretary trailed this this morning. The Prime Minister is chairing a hidden harms summit next week, which will look across the areas of police, victims and children. I am sure that will be brought up.

Chair: It would be very helpful to have more information about this from you. We have, in previous Home Affairs Committee sessions, heard considerable evidence about such things. Facebook closed groups is just one example of an area where we have heard evidence that action is not being taken to deal with crimes being committed and far-right extremism. We would like to know what you are doing about that, whether you or anybody in your Department has raised it with Facebook, and specifically what the remedy would be from the online harms legislation and what, in practice, it would be able to do about it.

Q545 **Tim Loughton:** Good morning, Ministers. I want to come on to the question of covid and child abuse, but first I want to come to Minister Dinenage on the subject of anonymity. If I want to set up a bank account and all sorts of other accounts, I must prove to the bank or organisation

who I am by use of a utility bill and other things like that. It is quite straightforward. What is the downside of a similar requirement being enforced by social media platforms before you are allowed to sign up for an account? This is an issue that we have looked at before on the Committee. Many of us have suggested that we should go down that route. I gather that it already happens in South Korea. You say that you are looking at it, Minister Dinenage. What, in your view, is the downside of having such scrutiny?

Caroline Dinenage: You make a very compelling argument, Mr Loughton. A lot of what you said is extremely correct. The only thing we are mulling over and trying to cope with is whether there is any reason for anonymity for people who are victims, who want to be able to whistleblow, and who may be overseas and might not want to identify themselves because they fear for their lives or other harm. There are those issues of anonymity and protecting someone's safety and ability to speak up. That is what we are wrestling with.

Q546 **Tim Loughton:** By the same token, you could have somebody with a fake identity who is falsely whistleblowing or pushing around propaganda, so it cuts both ways. I fail to see the downside of having a requirement that you have to prove who you are—not least because we know what happens when people are caught and have their sites taken down. Five minutes later, they set up another new anonymous site peddling the same sort of false information.

Caroline Dinenage: You make a very compelling argument. This is such an important piece of legislation, and we have to get it right. As I say, it is world-leading. Everybody is looking at us to see how we do it. We need to make sure that we have taken into consideration every angle, and that is what we are doing at the moment.

Q547 **Tim Loughton:** Can I come on to CSE? You both mentioned child sexual exploitation and abuse in your opening comments. As part of our domestic abuse inquiry, we have had evidence to the Committee that it has been increasing during the lockdown. We know that domestic abuse and child abuse go hand in hand. There is also evidence, certainly on the dark web, that groomers and child abusers are discussing and adapting to ways that they can take advantage of the lockdown to promote child sexual exploitation. It is an increasing problem, because in many cases we haven't got kids in school, where they can spot signs of what may be going on, and because kids are spending more time online if they are not in classrooms. What have your respective Departments done to make sure there is improved scrutiny, both from the Government and from the social media platform operators?

Baroness Williams: We are working with the NCA, the NSPCC and the UK intelligence committee both to assess the threat and to ensure that they have the resources they need to tackle this offending and to provide, obviously, the greatest protection for vulnerable children at this time. We know the scale of the threat on the dark web. We know it is significant, and we continue to leverage the unique capabilities of the joint operations

team, which is a combination of GCHQ and the NCA. This is to disrupt the most difficult, sophisticated and dangerous offenders wherever they operate, including on the dark web. During this time, we are uplifting the NCA's capability to disrupt those dark web offenders through the additional £30 million that we announced for CSEA in the spending round last autumn, in order to catch more offenders and safeguard more children.

Q548 **Tim Loughton:** Can I ask what that actually means? That additional money was absolutely pre-covid. What I have referred to in the last two months is a surge in CSE as a result of the circumstances imposed because of covid. You have said that the Government are assessing the threat, ensuring resources and uplifting NCA capability. What does that actually mean in practice, in terms of how children might now be safer because of the actions the Government are taking?

Baroness Williams: In uplifting that capability—in other words, having the resource to deal with it—it helps to make children safer. I have outlined briefly some of the funding streams that we have put in place, both for the NSPCC and the emergency support for charities, because charities are very important at this time. In terms of seeing an uplift, we certainly saw a huge increase in referrals of child sex abuse images to the National Centre for Missing and Exploited Children back in 2019—it was 50% in 12 months. We will probably know what the picture looks like during the lockdown only in hindsight, but all operational partners are absolutely alert to it. The point that I mentioned earlier about end-to-end encryption is the big impediment to identifying some of this stuff, both on the dark web and—

Q549 **Tim Loughton:** Without going back to encryption—I want to come to Minister Dinenage—you are referring to historical developments from 2019, not what has gone on in the last couple of months. Children's charities are doing an excellent job, but they are not enforcers. The additional money that the Government are rightfully giving to charities has not even been distributed yet. What is happening within the NCA and other Government enforcement agencies? Have we got more people monitoring? Have we got more officers out there? Have we got more people speaking to children? Have we got more people masquerading as groomers to entrap them? What practically is happening to make sure children are not in a more dangerous position because of the specific circumstances that coronavirus has brought on during the lockdown?

Baroness Williams: You talk about people entrapping child sexual exploiters and abusers, and that work is absolutely continuing. In fact, a recent development in Home Office capability has meant that we now have algorithms—you can imagine that the work that those people do is extremely traumatic—that know how to detect child sexual abuse images online, which makes the process far faster. There is always a human element to it, but that is No. 1.

You talked about the link between domestic violence, and child abuse and sexual abuse. I totally concur. I know, because I have asked the question

of them, that the police have been visiting not only high-risk potential victims, but high-risk offenders in the lockdown period.

Q550 **Tim Loughton:** Minister Dinenage, one of the things I am concerned about is that apparently social media companies during the coronavirus period have been cutting back on the human content moderation. That means that, on the face of it, there are fewer checks by the social media companies to try to root out and take down abusive material, child grooming attempts, and so on and so forth. The only positive thing that I can see, if it is a positive thing, is that, according to *The Times* yesterday, Facebook has set up a global censorship committee—whoopee—with some quite dodgy people on it, by the sound of it. Do you think social media companies are doing a better job or a worse job during the lockdown?

Caroline Dinenage: I am really pleased that you raised that, because it is something that we have concerns about. My boss, the Secretary of State at DCMS, met social media companies recently—obviously, digitally—to raise those concerns. We know that most companies use a combination of AI and human moderators, and most of the human moderators are scattered in different countries around the world, which have different covid restrictions. Some are socially isolated and are not able to get into work. As an aside, I suppose I am a little bit worried about the duty of care to some of those moderators, who have to deal on a day-to-day basis with some very distressing content. Because they are scattered around the globe, we are worried about whether the level of human moderation is sufficient. That is why the Secretary of State raised it with the companies very recently to express our concern.

Q551 **Tim Loughton:** What did they actually say? We have had the problem that, when we have had Facebook, Twitter and the rest of them in front of us, they would not tell us how many moderators they have got. It seems to be a closely guarded secret. They assure us that they have greatly increased the number of moderators, but they do not say by how many, where they are based and what they are actually doing. If there is one industry that shouldn't be affected by working from home, it is social media companies, which operate over computers in any case. Was the Secretary of State given any assurances that they have improved the moderation and taken on more moderators? Is it happening only in some far-flung part of the world and not in the UK, or what? We hear lots of platitudes from the social media companies, but we don't see much practical action.

Caroline Dinenage: I think we share your frustration on that. The human moderators are dotted around the globe, and different countries have different regulations in their covid-19 response. Just because your job is scouring the internet and looking for harmful content, you cannot necessarily do that from home, because you do not necessarily have the computer equipment to be able to do that. That is our concern. There is an additional concern around the mental and emotional health and wellbeing of those human moderators if they end up having to do that work from home, which is another thing to take into consideration. We have a

concern about the duty of care to those employees; we are frustrated by the lack of information forthcoming on that very issue.

Q552 **Tim Loughton:** The Government have a duty of care to victims and to consumers. Companies have a duty of care to their own employees; it is up to them to make sure that their employees are physically and mentally able to do the job of moderation that they are employed to do, and that they have the IT to do it. If they have not, then again, the companies are just paying lip service to the very important job of moderators. Isn't that right?

Caroline Dinenage: That is correct. As I say, because people are in different locations globally—

Tim Loughton: That is irrelevant.

Caroline Dinenage: It is very difficult for this to be something that we have any control over.

Chair: Baroness Williams, would you like to come in on that?

Baroness Williams: It might be helpful to the Committee if I say that we understand that Facebook has prioritised human moderators on some of the biggest threats, which will clearly include CSEA.

Q553 **Chair:** But you do not have any information from Facebook on how many moderators it currently has in place?

Baroness Williams: No, and I think it is important to say that, certainly in some of the operational work that we do in the UK, we would not give out that information, because it is operational. It may be the same for Facebook. I do not know the answer to that.

Chair: My question was whether you know how many moderators Facebook has. I think that is information that it should be providing to us or to the DCMS Committee. My understanding is that it has reduced or suspended some of its outsourced moderation arrangements, which also raises questions about how much of that is being outsourced in the first place.

Q554 **Simon Fell:** I would like to move on to the codes of practice in the White Paper. There are 11 harms for which the new regulator is expected to create codes of practice. There are more harms listed in the Bill itself, so why do the Government intend for there to be codes of practice for some of those harms but not for others? Is that the intention from the outset?

Caroline Dinenage: I think I need to clear up a bit of a misunderstanding about the White Paper. The 11 harms that were listed were really intended to be an illustrative list of what we saw as the harms. The response did not expect a code of practice for each one, because the codes of practice are really about systems and processes, rather than naming individual harms in the legislation. There are two exceptions to that: there will be codes of practice around child sexual exploitation and terrorist content, because those are both illegal.

For what you might call the "legal but harmful" harms, we are not setting out to name them in the legislation. That is for the simple reason that technology moves on at such a rapid pace that it is very likely that we would end up excluding something. For example, upskirting was something that three years ago was not an offence and now is—I do not think that most of us had even heard of upskirting more than two or three years ago. We want to make sure that this piece of legislation will be agile and able to respond to harms as they emerge. The legislation will make that clearer, but it will be for the regulator to outline what the harms are and to do that in partnership with the platforms.

Q555 **Simon Fell:** That is really helpful. On the harms that are already there, you say that you want it to be flexible and able to adapt, so as new harms are developed, what will be the process for the regulator to establish and build those in and create a framework for them?

Caroline Dinenage: That is a really important question. The regulator's work will obviously be ongoing. It will be setting out a sense of direction and a very clear set of expectations and guidelines for the sector. But there is also a responsibility on the sector itself—on companies themselves—to identify where they feel the harms are within their own content, to set out their own standards, expectations and duty of care, and to have a very clear complaints procedure and a way of being able to accelerate issues as well. So there are a number of different facets to that.

Q556 **Simon Fell:** If individual companies are setting out their own procedures, codes of practice and standards of care, where will the standardisation for that fall? If you have a number of different social media companies laying out their own codes of practice and they don't reconcile or perhaps have the same level of duty of care for their customers, do you expect the regulator to perform a function to range over that?

Caroline Dinenage: I think I may have misled and confused you there. It is for the regulator to set out codes of practice, but they won't be around individual harms; they will be around systems and processes—what we expect the companies to do. Rather than focusing on individual harms, because we know that the technology moves on so quickly that there could be more, it is a case of setting out the systems and processes that we would expect companies to abide by, and then giving the regulator the opportunity to impose sanctions on those that are not doing so.

Q557 **Simon Fell:** Moving on from that a little, I am a bit confused about the scope of the White Paper, where there are occasional suggestions that the regulator is going to be asked to provide guidance on whether content is appropriate. Can I check whether that is the case? Will the regulator be defining violent and hateful content—that sort of thing—or is that going to be left out of scope?

Baroness Williams: It is the codes that will provide guidance to companies on how to address things. Obviously, we will be publishing the interim codes of practice on terrorist use of the internet and CSEA, and it will be the codes that will provide the guidance to companies on how to

address that sort of content and activity. As Caroline says, it is a process point. But let's not wait for that point; I think it's important for companies to take action to tackle those harms now, but that is where the guidance will come from—the codes.

Simon Fell: Thank you very much. I have no more questions.

Q558 **Stuart C. McDonald:** I thank the Ministers for giving evidence this morning. I will also ask a couple of questions about scope, if I may. First, there have been reports that newspapers have been seeking some exemptions for online news media websites. What is the Government's response to those requests and what will their approach be to online news sites? I will go to Minister Dinenage first.

Caroline Dinenage: Obviously, we know that a free press is one of the pillars of our society, and the White Paper, I must say from the outset, is not seeking to prohibit press freedom at all, so journalistic and editorial content is not in the scope of the White Paper. Our stance on press regulation has not changed.

As for what has been in the papers recently, the Secretary of State wrote a letter to the Society of Editors, and this was about what you might call the below-the-line or comments section. They were concerned that that might be regulated. I think what the Secretary of State is saying is that, where there is already clear and effective moderation of that sort of content, we do not intend to duplicate it. For example, there is IPSO and IMPRESS activity on moderated content sections. Those are the technical words for it. This is still an ongoing conversation, so we are working at the moment with stakeholders to develop proposals on how we are going to reflect that in legislation, working around those parameters.

Q559 **Stuart C. McDonald:** But there is no suggestion that below-the-line remains unregulated. It is where that regulation should lie that is the issue.

Caroline Dinenage: Exactly.

Q560 **Stuart C. McDonald:** Another issue that has come up is that differences between what was said in the White Paper and the Government response to the public consultation have given rise to suggestions that search engines and other services that enable users to discover content might not be within the scope of the regulations. Is that correct?

Caroline Dinenage: Again, we are probably victims of the fact that we published an interim response, which was not as comprehensive as our full response will be later on in the year. The White Paper made it very clear that search engines would be included in the scope of the framework and the nature of the requirements will reflect the type of service that they offer. We did not explicitly mention it in the interim response, but that does not mean that anything has changed. It did not cover the full policy. Search engines will be included and there is no change to our thoughts and our policy on that.

Q561 **Stuart C. McDonald:** That is helpful; thank you. The Committee has

previously raised considerable concerns about the operation of algorithms and recommendation engines that social media sites use; particularly YouTube has caused us quite a lot of concern in the past. Will the regulator have powers to get involved in how those algorithms work? If so, how practically can that happen, because they are obviously very protective about them?

Caroline Dinenage: That is quite tricky, because algorithms are obviously commercially sensitive and commercially very valuable. The way I like to see it is that the legislation will basically force companies to take this responsibility for their algorithm. Algorithms are effectively a design choice, and as a result of that, they are a responsibility choice. If you are taking more risks with your algorithms, you are going to have to take more responsibility for the outcome of that.

The online harms legislation will demand much more transparency from companies as to how they are going about that. It also gives the regulator much more power to request explanations about the way an algorithm operates, and to look at the design choices that some companies have made and be able to call those into question. Of course, that will mean that the regulator has to have quite a lot of technical expertise. We need to make sure that they have that necessary expertise to be able to do that.

Q562 **Stuart C. McDonald:** Again, that is helpful, but to push a bit further, requesting transparency and asking questions is one thing, but if the regulator feels that algorithms are working inappropriately and directing people who have made innocent searches to, say, far-right content, will they be able to order, essentially, the company to make changes to how its algorithms are operating?

Caroline Dinenage: Yes, I think that they will. That is clearly something that we will set out in the full response. The key here is that companies must have clear transparency, they must set out clear standards, and they must have a clear duty of care. If they are designing algorithms that in any way put people at risk, that is, as I say, a clear design choice, and that choice carries with it a great deal of responsibility. It will be for the regulator to oversee that responsibility. If they have any concerns about the way that that is being upheld, there are sanctions that they can impose.

Q563 **Stuart C. McDonald:** You referred earlier, Minister Dinenage, to an uptick or spike in the revenge porn crimes that we have seen in the last couple of months. Does the White Paper have any implications for how that will be regulated in the future, and what can be done to try to protect victims better?

Caroline Dinenage: That is something that I am particularly passionate about. I used to be the Minister for Women and Equalities when we introduced the revenge porn helpline. During covid, we have seen a spike in calls to that helpline. Revenge porn is illegal, so it is something that Susan Williams might have thoughts on as well. We are very clear that

what is illegal offline is illegal online. Revenge porn is one of the online harms that we are concerned about.

Q564 **Stuart C. McDonald:** I get all that, but there do seem to be sites that almost operate as willing platforms for users. Is there the potential to use the forthcoming legislation to take tougher action against them, Baroness Williams?

Baroness Williams: That could be considered in the round. It is certainly something that has been highlighted during this period as not only a worry, but something that might be on the increase. Of course, as Caroline said, what is illegal offline is illegal online, so we have existing laws to deal with it. It will all be considered in the run-up to our response.

Q565 **Dame Diana Johnson:** I want to ask two questions. Earlier we heard reference to end-to-end encryption. I just want to be clear. Is it the Government's view that that would not be allowed in any legislation and that would be removed? Secondly, would the regulations cover private communications, and how would the Government choose to define what a private communication was? Those are my two questions to Minister Dinenage.

Caroline Dinenage: Susan will probably want to come in on the first point about end-to-end encryption. We don't see that encryption in itself is a bad thing, but we are very worried about end-to-end encryption for social media sites. To give you an example, in 2018, Facebook made 16.8 million reports to the US National Centre for Missing and Exploited Children, and the National Crime Agency estimates that reporting from Facebook will have resulted in more than 2,500 arrests by UK law enforcement, and almost 3,000 children safeguarded in the UK. They also estimate that 70% of Facebook's reporting would be lost if they implemented these proposals as they mean to do. It is not within the scope of our legislation to be able to stop them doing that, which is why the Home Office and the Department for Digital, Culture, Media and Sport have been making quite strong submissions to Facebook and have had meetings with Sheryl Sandberg at Facebook to try and articulate our very great concern about this.

Baroness Williams: Caroline has outlined some of the figures there. We have to be clear about certain things: the expectation that there will be a duty of care from CSPs to their users, and the fact that encryption in and of itself is not a good thing. Where criminals hide behind end-to-end encryption, it is a very worrying thing. We do not know what we cannot see, and that is a grave concern, particularly where children are concerned. As I mentioned earlier in relation to some of Facebook's takedowns and reporting of CSEA images, 83% of those 2 million takedowns were CSEA images. If that facility is end-to-end encrypted, not only will law enforcement not be able to see it, but Facebook will not be able to see it, either. I know that the Five Eyes partners are discussing it shortly. I know that there has been representation to Mark Zuckerberg from the Five Eyes countries. I would almost certainly guarantee that the

Prime Minister, when he does the online harms summit next week, will discuss it, because it is a very worrying development.

Q566 **Chair:** On that basis, does end-to-end encryption count as a breach of duty of care?

Baroness Williams: It is criminal activity that would breach the duty of care. Allowing criminal activity to happen on your platform would be the breach of duty of care. End-to-end encryption, in and of itself, is not a breach of duty of care.

Q567 **Chair:** Presumably, for this regulation to have any bite at all, they will have to be able to take some enforcement against the policies that fail to prevent criminal activity. On that logic, introducing the end-to-end encryption, if it knowingly stops the company from preventing illegal activity—for example, the kind of online child abuse you have talked about—that would surely count as a breach of duty of care.

Baroness Williams: I fully expect that that is what some of the Five Eyes discussions, which will be happening very shortly, will look at.

Q568 **Andrew Gwynne:** I want to come back on enforcement of the codes of practice. The White Paper envisaged that a suite of powers would be available to the regulator for enforcement. There is added complexity in that a number of companies who have a legal presence will be bound by those codes of practice, but quite a lot of internet operators are not based in the UK, although their services are available here. How will the codes of practice and their enforcement apply to all online services in the United Kingdom?

Baroness Williams: There will be scenarios where companies will be absolutely expected to report illegal content—I go back again to CSEA and terrorist content on the internet. There will, of course, be other scenarios where the balance is fine; legal but harmful is a more difficult area. Of course, there are also the terms of use, which we expect CSPs to abide by.

Q569 **Andrew Gwynne:** Presumably the regulations will apply to all content visibly available in the UK—is that correct?

Baroness Williams: Yes.

Q570 **Andrew Gwynne:** A provision is suggested in the White Paper to enable providers to appeal decisions by judicial review. What happens to that online content in the meantime? If the regulator deems it to be harmful but the provider does not, is that taken down until the judicial review is heard, or does it remain online?

Baroness Williams: I will defer to Caroline, but my initial thoughts are that we don't want to promote vexatious reviews but, at the same time, if something is harmful, we want it removed. Caroline, over to you.

Caroline Dinenage: My thinking is that it would have to stay down until any judicial review was concluded. The basis of comparison I have at the moment is where social media companies, for example, take down content because we have asked them to or they have concluded it is against their

own regulations. The people who have put up that content can appeal that decision, but until the appeal or review is done the piece of harmful content remains offline.

Q571 **Andrew Gwynne:** Is it justiciable and enforceable if the content is physically located abroad?

Caroline Dinenage: There is quite a lot about this in the online harms legislation that we are looking at. We have made it very clear that the enforcement powers we will be bringing in will be designed to ensure a completely level playing field between companies, whether they are based in the UK or not. Now, even though a lot of tech companies may be formed overseas, they do have a footprint—a registration of some form—in the UK. Regardless of whether they do or not, we want to ensure that the enforcement powers will cover everybody.

We have done an enormous amount of consulting on how we do that and what form any sanctions should take, but we are very clear that the regulator will have a range of enforcement powers, enabling it to take a whole suite of actions depending on the circumstances.

Chair: I am very conscious of time, and I know that Baroness Williams has time pressures. There are a few final issues that we wanted to cover, if we may test the Ministers' patience slightly.

Q572 **Ruth Edwards:** I just want to carry on with the issue of enforcement. Will there be criminal sanctions for non-compliance with the regulator, or for repeated or serious breaches of the duty of care?

Baroness Williams: My view would be that it depends on what the activity is. If the activity is criminal, then there would be criminal sanctions; if not, then of course you get into that grey area of legal but harmful. I am just homing in on the area of CSEA—stuff that is legal but potentially illegal. Some of the child sexual abuse images on, for example, Facebook may not actually appear like child sexual abuse images initially, but you click on a button and it becomes a child sexual abuse image. Well, for me that is illegal and reportable as well. So, I think it would depend on the issue.

Q573 **Ruth Edwards:** Okay. But for companies that, for example, repeatedly breach their duty of care, whether it is illegal or legal but harmful, and that perhaps do not show adequate respect for the regulator and for the laws they should be bound by, what kind of penalties are envisaged for those sorts of infractions?

Baroness Williams: The sort of penalties envisaged there are things like fines and warnings. But if something is criminal, it is not just a fine or a warning that you could be slapped with; obviously, it is a criminal offence.

Q574 **Ruth Edwards:** And what sort of scale are we talking about for these fines? Obviously, a lot of these tech companies have incredibly deep pockets and I cannot see that being slapped with a warning, or something like that, would be a huge deterrent for them.

Caroline Dinenage: I can probably help you with that. Obviously, we have not concluded the scale of the fines yet, but we have consulted on a whole suite of enforcement measures, and one of the things that we consulted on was senior management liability. We are still kicking around whether or not that is the way that we will go, but in other sectors we have found that similar provisions have definitely focused minds and driven culture change, and definitely improved regulatory compliance, for reasons you will understand. However, we need to understand what the impact of that would be in the tech sector. So, we will confirm our final position in the Government's response, but that is to give you an indication of some of the ideas we are kicking around at the moment.

Q575 **Dehenna Davison:** To return to the point that some of the companies are based almost entirely abroad and do not have that representation in the UK, I am struggling to understand how any enforcement action could be fully carried out there. If a company from a different country is not going to comply, I do not understand what specific powers will be in place in the new legislation to force them to do so, or to stop them from operating in the UK. Some clarity on that would be appreciated.

Caroline Dinenage: I can help with that. We are looking at a whole range of different things. Some of the lower-scale interventions might be working with advertising or financial services to tackle them that way. But the final sanction we have is blocking; we can block their site, which of course is quite a drastic action.

However, this piece of legislation, as I have probably bored you all rigid by mentioning earlier in this Committee, is world-leading. The eyes of the world are on us, to look at how we implement this. Other countries have done little bits piecemeal, but nobody has done anything quite as overarching as this, although a lot of countries want to.

So, online platforms that are seeking in some way to swerve this kind of guidance or regulation would be very misguided in doing so, because it will be coming soon to a country near them, and they would be better off identifying what their duties of care are, identifying what their standards are and looking at how they will best implement them.

Q576 **Dehenna Davison:** Are we specifically working with other nations' Governments to try and do—I guess—cross-country action on this sort of thing?

Baroness Williams: Yes, we work with, for example, the EU. The UK and France were first to set this up to take down terrorist content on the internet; we were instrumental in setting up the the Global Internet Forum to Counter Terrorism, to address that online. We have been at the forefront of a lot of initiatives.

Q577 **Dehenna Davison:** I have one final question. How will the regulator track the rise of new social media platforms—we have seen how TikTok has blown up over the last six months, for example—especially if they are coming from overseas?

Caroline Dinenage: The legislation puts the responsibility with the platforms to set out very clearly their codes of practice, standards and duties of care. The legislation falls very squarely at the feet of the companies themselves. If the regulator gets any complaints, it is able to gather information. If it gets what we might call super-complaints—a large number of complaints about a particular platform—that will certainly draw its attention. However, the regulator will also have the capacity to horizon scan—to see issues that are coming rapidly over the horizon towards us, and to predict areas where it thinks there might be concerns.

Q578 **Tim Loughton:** Can I come back to online fraud? We know that fraud is now the largest single issue that police cope with. It has increased exponentially, driven by online fraud, yet online fraud scams are not actually listed as harms in the Online Harms White Paper. Perhaps Minister Dinenage can comment on that, as well as the Minister from the Home Office.

Minister Dinenage mentioned at the outset that referrals to Action Fraud have actually been lower during the coronavirus outbreak, which goes against all the evidence and reports that we have been getting. How do we account for that? Is it genuinely lower because less fraud is going on, which we are sure is not the case, or is it that people have rumbled the fact that Action Fraud is pretty useless?

Caroline Dinenage: Online fraud and scams is a Home Office lead, but the White Paper recognised that there is already a significant programme of work across government to tackle online fraud and scams. This has been the subject of quite a lot of debate around the online harms legislation. Some stakeholders have called for fraud to be included in the scope of the White Paper, and we are still engaging on that at the moment ahead of finalising our policy.

The difficulty we have here, if I can be blunt with you all, is that we are trying with this piece of legislation to navigate a trade-off between making a really huge piece of legislation that encompasses everything and getting something delivered quickly that will put in place the protections that we know are needed right now. If you like, it is a bit of deliberation between speed and scale. Where there is already legislation and ongoing pieces of work that can protect people from certain harms, such as online fraud and scams, we are trying not to reinvent the wheel or duplicate.

Baroness Williams will talk more about this, but my statistics say that the number of cases reported to Action Fraud is slightly lower than normal. Up to 3 May, more than 1,300 covid-19-related frauds and cyber-crimes were reported to Action Fraud, with more than £2.8 million lost in those frauds. Clearly there is some covid-19-related activity, which is concerning. I do not know more broadly about other cases, because as I say, that does not fall under my ministerial responsibility.

Q579 **Tim Loughton:** Baroness Williams, do you think that online fraud has actually reduced during the lockdown period? What else could explain the failure of people to report it to Action Fraud?

Baroness Williams: I think the nature of crime and fraud has changed over the lockdown period. Caroline has given you the figures up to 3 May; up to 10 May, there were nearly 1,600 covid-related frauds and cyber-crimes reported to Action Fraud. There has been other activity: the National Cyber Security Centre, the NCA and the City of London police have identified scams falling into the broad categories of fake PPE, fake tests, phishing campaigns for bogus stimulus support and attempts to access home devices. They thwarted 2,000 scams in April, which is significant.

The NCSC launched the suspicious email reporting service just last week. In that time, 160,000 reports have led to 300 previously unknown phishing campaigns being taken down. We have also recently launched a gov.uk page on fraud and cyber-crime. So I think it has been well addressed over the period. It was identified before the lockdown period as an area that people might try to exploit.

Q580 **Tim Loughton:** Are you saying that the police, NCA and others have been more successful in detecting online scams and taking them down before anybody has become a victim of them? Have any of those people been prosecuted? The main complaint about Action Fraud is that fewer than 1.5% of referrals to Action Fraud end up with anybody being held to account or prosecuted.

Baroness Williams: What I can tell you, which is obvious from what I have said, is that there are more ways to report now and more ways to take down. Therefore, the overall the picture in terms of tackling fraud is a positive one.

Q581 **Tim Loughton:** I don't quite understand that. What has happened differently in the last two months to mean that, all of a sudden, these cases are not ending up with Action Fraud? Other than with the most serious and high-value cases of fraud, if somebody reports a case to the police then the police routinely refer it to Action Fraud, where it goes into a huge black hole and, where most cases never see the light of day again, certainly never lead to prosecution.

Baroness Williams: I take your point on that. We can do better.

Tim Loughton: Dead right!

Baroness Williams: I was speaking to James Brokenshire yesterday about it. I think we can do better on that.

Q582 **Chair:** Is there any plan to do better? It is all still really rubbish and this has been going on for some time.

Baroness Williams: It is something that I will take up with partners, particularly Minister Brokenshire. I can keep the Committee updated about the progress that we make. I take your point, Mr Loughton.

Chair: It would be great to have anything that you are doing on that. We have raised it in the past and it feels like it has deteriorated substantially since we last raised it, rather than got any better.

A quick final question from Julian Knight.

Q583 **Julian Knight:** Minister Dinenage, coming back to the here and now, if you like, and disinformation, research from the likes of the Oxford Internet Institute shows that disinformation is much more impactful when it comes through Twitter via a verified user—a blue tick. It is easy to get a blue tick; it is nigh on impossible to lose one. Should Twitter be much more robust in stripping celebrities, politicians and self-proclaimed journalists of their blue tick should they be found to be spreading harmful disinformation?

Caroline Dinenage: It is very tempting to immediately answer yes, without giving this due thought and consideration. My initial concern would be the difference between disinformation and misinformation. Disinformation is wilfully circulated by people who know exactly what they are doing. Misinformation can be shared quite innocently by someone who thinks they have read something important and passes it on.

If you are saying that we have to put a responsibility on everybody to check the veracity and accuracy of everything they are retweeting, for example, before they retweet it, then we will see an enormous amount of people—

Q584 **Julian Knight:** That is not what I am saying at all; I think you know that. I'll give you one example, if I may. I want to know whether you think this individual should have their blue tick removed, or whether you think Twitter should basically get their act together—I have alerted them to this. I was privy to a tweet from an Indian CEO who tweeted video footage of a Spanish hospital in the depths of the corona outbreak, suggesting it was the King's hospital in London. It was pointed out to him in comments that it was not—there were exit signs in Spanish and so forth. He acknowledged that it was not, but continued to allow that disinformation to stand. I alerted Twitter; they have done nothing. This is a steady experience; it is something that I, my Committee members and many parliamentarians come across regularly. But when you alert them, very little is often done. Should Twitter take action and remove the blue ticks from those who wilfully spread disinformation?

Caroline Dinenage: I can understand your frustration and anger at this. I think they would say the difficulty—I am certainly not here to defend Twitter in any way, shape or form—is how you differentiate somebody who is doing something knowingly and somebody who is innocently sharing something that they don't know is wrong. As you say, if it has been pointed out to somebody that it is wrong and they still refuse to take it down, that is an issue. The online harms legislation sets out very clearly that companies have to have a much more robust complaints procedure, and that the regulator can look at their complaints procedure and see how effectively it is operating. That is something to bear in mind.

Q585 **Julian Knight:** We are still waiting for online harms legislation. My hair may even get even greyer than it is right now waiting for the online harms legislation. For the here and now—right now, in the middle of this

outbreak—should Twitter be taking the blue ticks off those who spread disinformation?

Caroline Dinenage: I do not think that is for me to make a broad statement on in a meeting like this. If you want to send me any of the details that you have and all the correspondence you have—

Julian Knight: I was just asking for a general view from a Government Minister on this.

Q586 **Chair:** Finally, on the same theme—the things that the main social media platforms are still doing—we asked you about algorithms previously. We have previously raised in our reports, and directly with the social media companies, the YouTube algorithms and the way in which they push people towards extremism or towards madder and odder things.

This morning I did a search on YouTube for David Icke, and a few things came up. The second search I did was for 5G. When I went back to my YouTube homepage, the top recommended video for me, having just done those two searches, was a conspiracy theory video titled: "Sickness from 5G Cell Towers. Technology is Killing Us Slowly". That is YouTube promoting to me, on my homepage, some conspiracy theories. If I scroll down, there are plenty of BBC sites, mainstream news websites and so on, but the point is that, because of the first two things I searched, the YouTube algorithms have sent me more stuff to feed those kinds of concerns. Have you spoken to YouTube about their algorithms? Have you asked for information about the way their algorithms have worked, and do you have a plan in place to deal with the problem of the YouTube algorithms and what they suggest to people?

Caroline Dinenage: Not personally, although I speak to all the different platforms all the time. I will raise this again, but my officials are speaking all the time to the different social media platforms, which is why if you go on Twitter and search "5G in relation to covid-19", it will direct you the Government information. What you have articulated today is incredibly concerning, and I will raise it with YouTube.

Q587 **Chair:** Bear in mind that's not what comes up when I search; it's what is promoted to me to look at when I go back to my homepage. That is what YouTube's algorithms are promoting.

The frustrating thing about this is that we have raised this before; we have raised this directly with the companies. We have raised Facebook private groups before within our report to the Government, and also with the companies. We have raised Twitter anonymity before in our reports, and with the companies. We have raised issues around blue ticks and so on. Both our Committee and the DCMS Committee have repeatedly raised the specific issues and concerns about the way in which social media platforms operate.

We recognise that the Online Harms White Paper is extremely important, and that the legislation is important, but we are immensely frustrated that these individual things that platforms are doing are still causing harm and promoting harm, and making things worse, even when there

are things that each of those platforms could be doing to address it. So it has been slightly frustrating today that, on some of those specific things we have raised many times before, you have not got answers. I do understand this is difficult, but I think if there is anything more that you are able to send to us or say in any final words to us on how those things are going to be addressed, it would be very welcome.

Caroline Dinenage: I completely share your frustration and your sense of anger about this and I feel exactly the same way. That is why this inquiry from this Committee is incredibly important, because it gives extra power to our elbow when we are looking at how we are going to move forward with this legislation and make sure that we take on board all these concerns and we do what we can to address them.

My job is not to defend big high-tech businesses. My job is to, as I say, try to strike a balance and put myself in a position where I can look families in the eye and say that as a Government we are doing everything we can to protect them and their loved ones from harmful content. Any information that you can give me that will give me extra ability to be able to deliver on that, then I am very keen to see it.

Chair: A final word from Baroness Williams.

Baroness Williams: I would echo what Caroline says. Perhaps going back two or three years, now, when we talked about some of the steps that online CSPs could take in terms of being far more proactive about this sort of thing, it was like pushing water uphill. This is why we came to the position of the Online Harms White Paper and the Bill that will follow, because I, too, want to make the internet a safer place for my children, and exclude those who seek to do society harm.

Chair: Thank you very much for your time. I think if you are able to write further to us, to give us some greater reassurances that the online harms Bill will deal with those very specific examples that we have raised throughout this Committee session, and the kinds of harms that they promote on those particular platforms, that would be immensely welcome; but we are very grateful for your time. I am conscious that this evidence session has run longer today, and so we very much appreciate your time this morning. Thank you very much.