HOUSE OF COMMONS

Home Affairs Committee

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

Wednesday 3 June 2020

Ordered by the House of Commons to be published on 3 June 2020.

Watch the meeting

Members present: Yvette Cooper (Chair); Ms Diane Abbott; Dehenna Davison; Laura Farris; Simon Fell; Andrew Gwynne; Adam Holloway; Tim Loughton.

Questions 682 – 731

Witnesses

I: Commander Karen Baxter, Head of Economic Crime, City of London Police; and Graeme Biggar CBE, Director General, National Economic Crime Centre.

II: Susie Hargreaves OBE, Chief Executive, Internet Watch Foundation; and Robert Jones, Director of Threat Leadership, National Crime Agency.

Written evidence from witnesses:

– Written evidence from Internet Watch Foundation

Examination of witnesses

Witnesses: Commander Baxter and Graeme Biggar.

Q682 **Chair:** Welcome to this evidence session of the Home Affairs Select Committee. As part of our ongoing work on the Home Office response to coronavirus and wider issues, today we are looking particularly at issues around online crime, online fraud, and online harm and abuse, particularly during the coronavirus crisis but also more widely.

We are very grateful to our witnesses for joining us today. Welcome to our first panel: Commander Karen Baxter, the Head of Economic Crime, City of London Police, and also Graeme Biggar, the Director General of the National Economic Crime Centre. I welcome you both to our evidence session this morning.

Can I start by asking you what changing patterns you have seen in online fraud during the coronavirus crisis?

Commander Baxter: Ever since the beginning of coronavirus, what we have found is that in the first two weeks there was an initial drop of 50% in calls for service from victims. After that happened, we were very quick to re-establish our provision of the Action Fraud service to victims and to the public. We found that the trends in how victims report have changed. For example, we have had about a 30% decrease in telephone calls but had about a 30% increase in online reporting. Overall, we now have a 7% increase at the end of May in comparison to where we were pre-Covid.

As you would expect, the types of crimes that we are seeing are slightly different because people are living differently as a result of Covid. Just to give you a flavour of that, we have seen a significant drop in computer software crime. The reason for that, we believe, is because we can track it to boiler rooms and illegal call centres in India. When India went into lockdown, we saw a significant and very sharp drop-off in that type of fraud.

We are seeing dating fraud pretty much remain steady, with a slight increase. We have seen a significant increase in shopping and online auctions, about a 46% increase in comparison with the pre-Covid level, and that is very much because people are now living their lives online, doing their shopping online, and that is something whereby they can become quite susceptible.

As you might expect, with the slowing down of the economy we have had a decrease in mandate payment diversion fraud. Interestingly, while we had a drop overall in courier fraud—and you might remember we did an operation on courier fraud at the beginning of the year—we did see, I think, in the region of 21 arrests for courier fraud which, in effect, were contact offences where criminals were targeting older people, meeting them and taking substantial amounts of money from them.

Graeme Biggar: Just to echo everything Karen has said, and then just to add a couple more points. I think we have seen fraud in this period fall into three broad categories. There have been the frauds that are specifically taking advantage of Covid, so the sale of fake test kits or fake personal protective equipment, or even investment frauds that try to use the fact of Covid as a hook to lure people in. The same thing happens in romance fraud and various other frauds.

We have then seen what has been happening with public sector spend, so that is another big area to mention. It is fraud against the public sector, so two types there: the huge expenditure the NHS and other parts of the public sector have been trying to do to buy ventilators for the NHS, and then personal protective equipment more generally. There are real opportunities for fraudsters there, and we have been working very closely across the public sector to try to combat that.

Also, the stimulus packages that the Government have introduced is an enormous amount of money. Like any enormous amount of money, particularly coming out from the Government, there will be attempts from fraudsters to get into that as well, so we have seen a fair bit of that.

The third category is just what happened—and Karen talked about this—to fraud generally during this period. It is probably worth mentioning that the very specific Covid-related frauds are only 2% or 3% of the total number of frauds that are reported to Action Fraud. The vast majority of fraud has just carried on. There was a dip and then it has risen, as Karen has mentioned. We have the very specific Covid frauds, a small proportion, and then just frauds generally, which dipped and then returned to the trend that we had before, a trend that has been increasing.

Q683 **Chair:** In terms of the scale of the numbers, Action Fraud has reported more than 2,000 cases of Covid-19-related frauds with total losses of £4.6 million. Are those the most up to date figures?

Commander Baxter: They are. The figure I have here is 2,130, and we have in the region of £4.9 million losses in total.

Q684 **Chair:** Just to get a feel for this, of those, say, 2,000 cases, how many of them have been referred to police forces? How many of them have been investigated?

Commander Baxter: Of those 2,130 cases, 1,682 were defined as crime reports and a total of 350 were disseminated to forces for investigation. Some of those were pursue investigations and others were protect. What I would say is that all of the cases in terms of Covid-19 were reviewed. Some of those were then disseminated quick time for very quick action. For example, we had a number of cases where we believed fake testing kits were being used and were extremely harmful, so we had quick deployments in respect of those.

We had other cases where we had large-scale smishing and phishing offences taking place, which were targeting a larger number of individuals.

I think we had 16 of those in total. So far we have two people charged, and we have 17 further people now ready for charging. In total, we had 47 arrests and they are being progressed through the criminal justice system.

Q685 **Chair:** So, 47 arrests. There is always a time lag in these cases anyway. We start from 2,000 cases that have led to 47 arrests?

Commander Baxter: Yes, that is correct.

Q686 **Chair:** Only 350 of the 2,000 have been referred to police forces. Of those 350, how many of them have actually been investigated? Certainly, when we have taken previous evidence around fraud cases, we have found that only a tiny proportion of the cases actually referred to police forces ever got investigated.

Commander Baxter: I do not have specific information on how many of those have been investigated. What I can say in terms of how we dealt with the Covid-19 crisis is that we adopted Project Etherin. We had daily intelligence and information briefs with the forces involved. The Covid-19 fraud investigations were taken as a priority by the economic crime investigators in each of the respective 43 forces.

In terms of the uptake of investigations, there was a greater uptake of investigations during the course of the pandemic. I do not have the outcome of those cases. A number of those cases are ongoing, as I said.

One of the reasons why cases are ongoing is that, while we made arrests, the Covid-19 social distancing issues prevented us from actually bringing suspects into custody unless it was an absolute necessity. Therefore, you have a lag when we have gone out, arrested, de-arrested, seized the evidence and are now putting that through the forensic examination, hence why you have two people charged and 17 people about to be charged.

Q687 **Chair:** Do you have the systems in place so that within, say, three months, or however long, you will have the detail on how many of those 350 cases have been pursued, or do you just not follow it up once it is passed on to forces?

Commander Baxter: In respect of Covid-19, we have systems in place to follow that up. Obviously, at the same time that Covid-19 was happening, we had other frauds that were being reported. We have about 7,000 of those reported on a weekly basis. It is much more difficult to pursue that volume. However, what we have been working with in the last six months is about a better sense of tasking and also a better sense of that information coming back. It is extremely important to us that we get that information. It is important to you, and we are working with forces to improve that system.

Chair: Okay. We will come back to that shortly.

Q688 **Andrew Gwynne:** Investigating these crimes is obviously one side of the equation. The other side is clearly ensuring that these frauds do not happen in the first place. I would like to get a sense from you of what was being

done and what is being done to prevent these frauds from happening in the first place.

Graeme Biggar: Absolutely right, and not enough is the overall answer in this country to try to stop fraud happening in the first place and then tackle it. Simon Fell will know that from his previous jobs as well.

We have been working closely with City, with the Home Office and with loads of different partners on fraud to try to work out what we need to do to change the way we are tackling fraud in this country. We think there are basically five things that we need to do. The first is to put a clearer leadership and governance structure around how we have been tackling fraud. City has done a good job on that with policing, but we are trying now to reach out to the rest of the law enforcement community, to regulators, bringing in the private sector more as well and work with central Government. We need leadership from the Home Office on that to take a central departmental lead, and then from the National Economic Crime Centre on the operational level working with all the partners, so that is leadership and governance.

The second thing we need to do is to have a stronger intelligence picture. That has not historically been strong on fraud. We have some really good snippets of information. Cifas gathers some really good data, and City do from Action Fraud reports, but we have not historically pulled it together into a single, really good picture of the intelligence. We have not collected on it using covert tactics in the way that we should. We have not pulled in international data. We have not pulled in private sector data in the way that we could and should, so there is a lot more we can do there.

A better intelligence picture can then allow us to do two other things better, the third and fourth areas: one is pursue and the other is protect, which goes to your point, Andrew.

Pursue first, we just do not have enough people to investigate fraud in this country. It is now the single largest crime type. It is 35% of crime reported through the Crime Survey for England and Wales. It is 10% of crime reported into police, and we have 1% or probably slightly less than 1% of policing devoted to it. We do not have the resources to do that at the moment. We need to change that. We agree with the previous Committee's recommendations on this. You need to base it around regional centres and build up regional investigative centres. There is also a need for a national investigative capability in City and the NCA, so I think more investment in pursue.

Fourthly, penultimately, protect, going to exactly your point. There are two things we need to do there. One is communicate to the public much more effectively around how we get them to avoid scams. We have been doing a lot on that, but we need to join it up better and make it more powerful. The second is to design out fraud in the first place, which we can do in a range of sectors. The financial sector is an obvious one, and we have done

a fair bit with them. They have done a fair bit themselves, but there is a bunch of the rest of the private sector that we need to involve, too.

Finally, as well—where we started—we need to get the system of reporting for the public, through Action Fraud into the National Fraud Intelligence Bureau at City, out to local policing to work more slickly than it is at the moment. That needs a bit more investment. Karen and her team are working hard at improving that and have made some good progress.

Those are the five pillars of our plan to improve fraud. That is what we have been discussing with the Home Office. That is where we think we need to secure investment through the next Spending Review to help get this country into a better place in tackling, as I said, the biggest single crime type we have at the moment.

Commander Baxter: There are a number of things that we do to prevent people from becoming victims in the first place, and it is an extremely important part of our business. The first thing is that we risk assess the calls that come through, and we risk assess the information we have. That is about identifying those who are the most vulnerable. For example, since October 2016 we have dealt with 1,300 extremely vulnerable, suicidal people who have contacted the call centre. We have procedures in place to deal with those and have them dealt with immediately by each of the respective forces.

Outside of those people who are in a position where they may self-harm, we have other individuals who are particularly vulnerable. Those, for example, are older people, perhaps subject to courier fraud. That is why we identified courier fraud as one of the key operations that we ran in January this year, where we arrested over 44 people and charged a number of people. We look at prioritising those types of offences.

The second thing is about our protect strategy. We have learned from the cyber network that, in terms of Cyber Protect, there is a lot that we can do about educating the public and making them aware of those threats. We have adopted those processes. We use some of the Cyber Protect network to disseminate broad protect messaging. We do that on a daily basis. During the Covid-19 period, we reached 43 million people with protect messaging.

We were also able to identify certain fast-time intelligence and get that out in a matter of hours. You may be aware of the Tesco voucher fraud. We were able to work very quickly, within a space of about two to three hours working with Tesco, to highlight that to the public; therefore, preventing people latching on to those types of messages.

The third issue is about proactive use of intelligence. One of the key areas that we have identified is the issue of smishing and phishing where, on an industrialised scale, we have individuals who will be sending out information to your phones, to your laptop, and will be targeting individuals.

For example, we have targeted those individuals. We had an industrial smishing case on 14 May. I can give you an example of what that actually means. We first seized a number of items and devices. When we looked at that, we tested and we found 588 texts, and this is on one device. In the next 80 minutes there was an average of seven messages per minute that were sent out. In the next 75 minutes there were 670 messages sent out at eight messages per minute. We found 261 victim details on one phone. We found what was assessed by the banking industry to be an estimated £150,000-worth of crime attached to that one phone. In those cases, we seized a number of phones and a number of other devices. It is about prioritising where we deal with the intelligence and looking at those individuals who are targeting individuals on an industrial scale.

The final thing is that we work with partners. Policing is one part of what I call the big system in how we deal with fraud. There are many assets across that system, and different assets have different benefits. For example, as part of Covid-19, we expedited the use of the NCSC phishing tool. We brought that forward from June to April. I am really pleased to say that we have identified over half a million e-mails, and I think we have taken down 3,700 of those. That is about industrialising.

Finally, we work with other law enforcement partners in other jurisdictions. I have already mentioned India. It is one of the key areas where they target the United Kingdom in terms of computer software. We have worked with law enforcement in India to close down those centres and, therefore, impede the action of criminals in those countries.

Q689 **Andrew Gwynne:** I think most people watching these proceedings would be quite surprised to hear that this is the single largest crime type, yet only 1% of policing is associated with it. I just wonder, given that you must have been alert to the threat of the Covid-19 pandemic in increasing this area of crime—we have heard, for example, from the World Health Organisation that very early on there were fraudulent e-mails impersonating the WHO back in early February—that more resources could have been put into this area in anticipation of there being an upsurge in this kind of crime.

Commander Baxter: The first thing is that no resources actually moved out of fraud in terms of our capability and capacity to respond. We were able to identify that through the national tasking process, which we work through with the National Crime Agency.

The second thing is the priorities for policing. While the vast majority of crimes did reduce, there were other issues that policing had to deal with in terms of vulnerability, people at home and the social distancing issues, so there were a number of other competing priorities. I would say that, while we did not increase the resources, we did bring together the assets across the National Economic Crime Centre with policing. We had a much better co-ordinated response to Project Etherin, which was the NECC response to Covid-19, than I would say we would have had last year.

We have moved in the last 12 months, as a national lead force, from what has been more in terms of policy to co-ordinating deployments—physical deployments, pursue deployments—and those operational impacts. I think we have moved significantly in the last 12 months, and we are using the regional organised crime units and the 43 forces in a much better co-ordinated way to address the targets and the criminals who are perpetrating these crimes.

Graeme Biggar: If I could just clarify, fraud has not gone up under Covid. Covid frauds have obviously become a thing that they were not before, but fraud actually reduced in the first weeks of Covid. It is now back up to the original levels, just to clarify that point, and the 2,000 Covid frauds that Karen mentioned are within that very large total figure.

We have, though, swung a lot of resources into this from other bits of fraud, so we have really focused on the Covid frauds. Karen mentioned Op Etherin, which is the co-ordinating campaign we have had, bringing together not just policing but other law enforcement partners, the private sector, National Trading Standards and some charities as well, to try to make sure we do three things. One is to have the best understanding of what is happening, so pulling together the data, the anecdotes and the evidence from all the different people who are gathering information on this, and then explaining that back out to the community so that they can help put the right protective measures in place.

Second is to co-ordinate as best we can—and City does a lot of this—the response to those crimes that are being committed. Then, thirdly, getting the comms in the right place, and Karen mentioned some of that as well. There have been a lot of comms that we have put out, that City has put out, National Trading Standards and the FCA, to try to warn people about what is out there and how they can protect themselves.

Q690 **Andrew Gwynne:** It comes, lastly, to your point, Graeme, about leadership from the Home Office and having those resources to be able to pursue and protect. You mentioned the Spending Review, but have any discussions been taking place with Ministers and officials in the Home Office to ensure that, prior to the Spending Review, those resources are available and there is that leadership to be able to tackle not just these frauds during Covid but beyond the pandemic?

Graeme Biggar: Yes, basically. I came into post just over a year ago, and fraud did not feel like the biggest priority within economic crime at that point. People were more focused on international money laundering. It is felt that there has been a real general swing, which I completely support and have pushed, into looking more at fraud, just given the scale of it and the way it affects people That has been in alignment with the various different Ministers that we have had in the Home Office during that time including, absolutely, the current Home Secretary and Security Minister. They are very focused on how we can improve that.

There are more people in the Home Office looking at fraud now than there have been previously. We have been discussing with them not just what we can do in the Spending Review but also what we need to do right now. On that point, we are benefiting from the investment we have had into the NCA, and a little bit into City as well, from the package around illicit finance, which Amber Rudd announced a couple of years ago when she was Home Secretary. We have had more money in there, which has allowed us to build the National Economic Crime Centre.

We are only a year and a half old at the moment. We have been building the national data exploitation capability within the NCA to allow us to do much better things with big data and search across it. We have been building up the national assessment capability within the NCA to allow us to do better assessments of what is happening across the board, and we are gradually, although a bit slower, building up our investigative capability, too. That has been for economic crime in the round, but we have been swinging more of that into fraud in the last year and the last few months.

Q691 **Simon Fell:** Just to declare an interest up front: prior to the election I used to work for Cifas, the counter-fraud organisation that chairs the Joint Fraud Taskforce that both Graeme and Karen, at least to my knowledge, still sit on.

Can I start with a simple question to you, Commander Baxter? What percentage of frauds do you think are generated from social media at the moment?

Commander Baxter: It is extremely hard to say specifically what clear percentage is generated from social media. What we have in Action Fraud is the victim intelligence, the victim reporting. What we have seen is that a minimum of 12% of the victim reporting clearly refers to social media. We would say that, when you look at the cases, it is probably more than 12%. What we do know is that 86% of fraud has some form of cyber aspect.

We are acutely aware of it. I cannot give you any more specific information but, at an absolute minimum, it is 12%, and we believe it to be more than that.

Graeme Biggar: I would just add that it is very hard to get this figure right. We are all conscious that this is an area we need to get into a lot more, which we have been doing alongside Cifas, both to understand the extent to which social media companies and social media are part of this and then to engage with them to try to reduce the way that happens.

Q692 **Simon Fell:** You have led me nicely on to my next question. Do you think social media companies should be doing more?

Graeme Biggar: I think everyone should be doing more on fraud. I do not think we are tackling this as seriously as we need to across the entire country. That is absolutely in my organisation as well as everywhere else,

but definitely in social media companies, too. My previous job was on terrorism, and I was always asking them to do more on terrorism as well. There are lots and lots of demands on social media companies, and I recognise that, but it really matters and they do need to be doing more.

We are seeing messages circulated on Instagram and Facebook that are advertising things that turn out to be scams. We are seeing search results coming up on Google that put very prominently investment opportunities that turn out to be scams. They are not being taken down quickly enough. A whole series of things need to be done in the social media sector as well as in other sectors—the banking sector, the retail sector, the insurance sector and so on. Absolutely, yes, they should be doing more.

Commander Baxter: I agree with everything Graeme has said. In terms of social media, we are making inroads by working directly with some of the social media platforms through some of our funded units, where we can engage very quickly and get some of the sites taken down, but I agree with Graeme that more needs to be done right across the board.

Q693 **Simon Fell:** Yes, I take a view that prevention is obviously key but so is reporting, so that when they spot something going up they get that to you so you can action it. I am curious to draw more out as to what you think a solution might be for social media. What would you like to see from them?

Commander Baxter: You have got me in a spot there. I think stronger engagement is really important. We find in policing, on an operational basis, that when we ask for information it often feels like a difficult road to get that information. Quite often the information sits in other jurisdictions and unfortunately, even though we ask for that information, we often find that the case is closed. It has been through court before we get that information coming back to us, if we get it at all, so there are significant delays, often very significant barriers, in receiving the information for an evidential purpose. I think those need to be ironed out in some respects.

The second thing is that how we deal with fraud is not just within law enforcement, and you will know this from Cifas. How we deal with fraud is very much a public-private partnership. How we access the data and how we build trust is extremely important, because I think there is a suspicion or a thought that policing and law enforcement just decide to trawl through accounts and trawl through information because we have nothing better to do. Policing has not been strong in showing its accountability and its transparency for that.

There are very clear guidelines on how we operate, on what information we ask for and on what data we wish to be shared. A lot more needs to be done on building trust, building those partnerships, expediting the flow of information between services, and understanding that at the heart of all of this there are serious harms taking place. There are people losing perhaps their entire pension funds, significant amounts of money, which has a significant impact on their welfare and health in the long term.

I think all that narrative has simply been lost in another argument about the protection of personal data. I would like to reassure the public that we do not ask for personal data unless we really have to, and we do not ask for it unless thresholds have been met.

Graeme Biggar: There are three broad areas on which we can do more with the social media companies, all of which we are doing a bit on but we need to be doing more. One is data sharing, and in fact Cifas and the Joint Fraud Taskforce have been piloting some work with one of the big social media companies—I cannot remember whether we have said publicly who that is or whether they have agreed to it, so I will not mention it now—to better understand the data they have and how we can use that to help spot when scams are happening, the language that is being used.

There is more we could do on data sharing. There is also more they could do in communicating the risks of scams and allowing scams to be reported online. Facebook and Google do a bit of that. Google just launched a new comms campaign around it last week, I think, but there is more we can do on that.

Thirdly, as Karen mentioned, there is also taking down sites and accounts that are being used for fraud, which is not as slick as it could be at the moment. The FCA has been working quite hard with Google to try to get investment scam websites taken down and to stop them being put at the very top of Google search results in a kind of paid ad way. We think this is something that Google makes money from. Fraudulent websites are paying to have their search results put at the top of the string that comes up. They have not had as much success with Google there as they would like, and I think that was reported in *The Times* in February.

There is more that could be done there, both getting those sites taken down and then helping make more prominent the counter-fraud messages, be they from Government, from law enforcement or ones that the social media companies come up with themselves.

Q694 **Simon Fell:** Going back to something you mentioned, Karen, obviously most of the time there is a victim sitting behind the fraud. These are often quite harrowing cases, and you mentioned pension scams and all that. Do you think online fraud should sit within the proposed Online Harms White Paper?

Commander Baxter: Without a shadow of a doubt. We see the harm that fraud causes to people, individuals, families and the wider community. It absolutely needs to be in that paper. We were disappointed it was not included.

Graeme Biggar: I absolutely agree with that as well. We lobbied hard for that. We understand the challenges DCMS and the Home Office face. It is now a matter for Parliament, but we would strongly support that.

Q695 **Ms Diane Abbott:** Commander Baxter, I think a member of the public

listening to you just now would be surprised that you were not able to be definitive about the percentage of fraud that uses social media. If I remember, you said it is about 12% if you go by victim reporting, but it is probably higher. Are you telling the Committee there is no definitive way of establishing the amount of online fraud that uses social media?

Commander Baxter: What I am saying is that the use of social media across fraud by criminals covers a range of issues. Action Fraud will take information from victims, and we can tell that the 12% is a minimum because it is in the records that the victim has said they have been involved in social media. The second thing is that we know certain types of fraud—for example, dating fraud—very much rely on social media platforms.

That is just one part of intelligence information that we have. We work very closely with the banks, with UK Finance, and what we have identified in working with the private sector is that they also have identified where social media is used. You will have heard of the term "herders" who set up large networks in which they launder money through bank accounts. We know that the herders will recruit mules, and these are individuals. One individual will recruit perhaps 30 to 40 other people on various social media platforms and will use those people to launder money through their various accounts.

That is only two parts of the sector, and each of those bits of information covers a wide variety of sources, so I cannot be definitive. I would like to be definitive, but the analysis of that would require significant investment. That is why we have been working with the National Economic Crime Centre on developing a fusion cell. It is about bringing all the intelligence between the private sector and the public sector together. It is about a quicker understanding of what the information you have just described says to us and, more importantly, what we can do with that. That needs investment, and that is why we would like to get that investment going forward to develop that analytical response.

Q696 **Ms Diane Abbott:** So there is a way of establishing definitively how much online fraud is done via social media but you do not have the resources to do it?

Commander Baxter: I think there is a way that we can better identify and have more clarity about how much social media is involved in the fraud offending landscape. I am not sure we would get to a definitive. When we look at online, when we look at the dark web, when we look at social media platforms—

Q697 **Ms Diane Abbott:** You could do better than you are doing now, couldn't you? Are you saying that you do not have the resources?

Commander Baxter: We have put forward a spending proposal that outlines what we think, in the first instance, in terms of a fusion cell, which is what we have already established. We have started a fusion cell and we are looking to build that fusion cell, which is about bringing private and public information more closely together. As part of the National Economic

Crime Centre, we have the intention to build that at pace over the next six to 18 months.

Q698 **Ms Diane Abbott:** Would you like to say more about what you think social media companies could do? You talked about the difficulties in relation to getting information—the delays and the difficulties with barriers. Would you like to say more about that?

Commander Baxter: I probably covered it quite extensively in my previous response, in that when we ask for information from law enforcement, we would prefer that the information comes through in a timely fashion. That information can then be analysed and presented before the courts. Quite often we will make an application to various social media companies and it might be 18 or 24 months before we get that information back. You will know that delaying justice for 24 months, three years, four years, is not good justice and is not good for victims. We would certainly prefer that that information is shared with us at a quicker pace.

Q699 **Ms Diane Abbott:** Is there anything the Government could do to make social media companies respond to you promptly?

Commander Baxter: Obviously, whatever influence the Government could bring to bear with social media companies in encouraging them to do that better, if not mandating them to do it, would be welcome. What we need to do is think more broadly around how that whole system works.

When you think of the Fraud Act, it was written at a time before we had all these issues of social media. We have had a significant increase in digital information and digital intelligence and, certainly, all that information is now being used more widely across the courts. What I would suggest is that the legislation probably needs to change to keep us updated and to respond to where we want to be in 2025 and 2030.

Q700 **Ms Diane Abbott:** Do you think legislation is probably the best way to get meaningful co-operation and to speed up data sharing?

Commander Baxter: Legislation is one way, and it is certainly one aspect of what we collectively, as the counter-fraud community, need to consider going forward. It is time that we—

Q701 **Ms Diane Abbott:** What would be the other aspects, if not legislation? We have talked about the Government using their influence, but that does not seem to be working.

Commander Baxter: That is a matter for the Government. I would say that anybody with influence can start to change the culture within which we work. Policing itself is working very hard to change the culture. It is proactive in terms of its engagement with social media companies. We have had some reasonable successes with social media on a small scale, where we have dealt with them directly through our card crime unit. We work with them as trusted partners, but that is a small-scale operation. We need to increase that, and we need to increase the trust.

I go back to the first issue I discussed. When we ask for information around data sharing, around social media information, around sites, it is because generally—and it should be right—there is a necessary, proportionate and justified reason for us to ask for that. We are not asking because we are interested in people's personal lives. We are asking because a crime has taken place, and in most cases because a very serious crime with serious harm has taken place.

Q702 **Ms Diane Abbott:** No one on the Committee thinks you are asking for information from the social media companies for trivial or casual reasons. What I am trying to get to is what the Government need to do, and it seems to me that what I am getting from you is that the Government need to look at the legislation.

Commander Baxter: I think, collectively, the legislation and other aspects. We would be open to all other aspects of influence and negotiation with social media sites taking place going forward. That will strengthen law enforcement and how we protect victims, particularly in terms of fraud and the online harms.

Graeme Biggar: We have already said that we would support economic crime and fraud being part of the Online Harms Bill as it comes through Parliament. That would be one of the legislative solutions.

Secondly, there has been one already in the UK-US data access agreement that was signed, I think, last autumn by the Home Secretary in Washington. That will make it easier, when it is fully implemented, for us to get information more quickly out of social media companies that are headquartered and have their data stored in the US, so that is a really big step that the Government took and negotiated over the previous two or three years. In fact, legislation went through Parliament to enable that.

Thirdly, as we said earlier, there is definitely more that social media companies can do but, as we also said, we are not in the right place. Your initial question is absolutely right in terms of our understanding of what is happening and the data. We need to build up our evidence base and understanding, and then we need to engage more with social media companies. It would not be fair for us to sit here and say that we have done everything we possibly could and that we are meeting a brick wall. There is definitely more that we could do, and then more that they can do on the back of that.

Q703 **Ms Diane Abbott:** What could you do further to build up the data? The first step in taking action is always to have the information and, as matters stand, I am hearing a sort of inconclusiveness about the proportion of online fraud that uses social media.

Graeme Biggar: Yes, the data is really mixed. On reports into Action Fraud, as Karen mentioned, 86% have some internet dimension, not just social media. If you look at the data collected by the Crime Survey for

England and Wales, it is 54%. That is 3.8 million, so it is a much bigger figure than the one Karen is talking from.

The overall data around fraud is really varied, and we do not have a good grip on this yet. That is part of what we want to do better. Within that you have the question of what you count as being a social media-enabled crime. The definitions can vary, but we absolutely need to get better evidence on that. That will improve our understanding. It will allow our engagement with social media companies and our communication to the public to be much more targeted, so I completely agree with your initial point.

Q704 **Tim Loughton:** I am afraid I am getting a bit of a sense of déjà vu listening to proceedings so far. Of course, the Committee looked at this in the "Policing for the future" report back in 2018, and it was interesting to hear Mr Biggar refer to a five-point plan. Great. Many of those points were covered in our report, and now they are just a plan. There are plans to talk to their partners, plans to have various conversations, but not much action.

We made some specific criticisms in that report, not least the apparent inability of Action Fraud to prosecute anybody. The figure from that report was that, "Of the 1.7 million offences committed annually, it appears highly unlikely that more than one in 200 victims ever sees their perpetrator convicted." Fraud continues to be the biggest part of crime that the police are dealing with. It has been the fastest growing, and we hear again that fewer than 1% of police officers are dedicated to it. When is this going to stop being just conversations and plans? Are we going to see some real action where fraud is properly investigated, prevented and researched, and where people are apprehended, charged and prosecuted for it, rather than it just becoming an increasingly growing problem?

Commander Baxter: The first thing I would say is that Action Fraud is not an investigation centre; it is a central reporting conduit. The purpose of having a central reporting conduit is that all of the information will come together around a fairly complex type of crime, and we are then able to better understand, across all of the victim reports, what the intelligence tells us.

The second thing is that we rely on and disseminate to 43 forces, 43 chief constables and 43 PCCs responsible for investigating fraud. In the last 18 to 24 months, I have seen a significant change in, first, the awareness across 43 forces of the importance of investigating fraud. That said, there are, however, competing requirements. In the last 10 years, we have had a reduction of 20,000 police officers. We have had significant reduction in budgets. That has all had quite a significant impact on policing. It has had a significant impact not just on pursue and arrest; it has had a significant impact in terms of prevention.

The number of priorities competing for a minimal set of policing resources is growing. We have priorities in terms of physical violence, sexual crime, child sexual exploitation and county lines. Unfortunately for victims of fraud, for too long the narrative has been that financial harm does not quite

equate on the same level as physical harm. As a result, not every police force in the country would have fraud as part of their policing plan.

As part of the HMIC report, we have asked and pursued all of the forces to consider that. We have also pursued it with 43 police and crime commissioners. That is the first thing. There is a landscape behind this that does not always encourage pursue in the way we would want, certainly now and in the future.

The second thing is that we have changed in the last 12 months. We have worked with the National Economic Crime Centre. We have moved from, in some ways, a policy-based approach to fraud, and we have strengthened our pursue approach. That is about increasing the number of arrests. Project Otello, which is a 12-month campaign looking at a number of types of fraud, has seen certain successes. That was on the back of the national tasking in December.

In January we launched Operation Radium, which is about addressing courier fraud. Courier fraud is extremely important to policing, because it is a contact offence with victims—with older, vulnerable victims—where criminals will target them for large amounts of money. There is always a risk of physical harm in that as well. Over the space of four weeks we made about 44 arrests. I can get you the figures, I just do not have them off the top of my head.

We have looked at increasing our arrest and our pursuit of criminals. We have also invested in a joint money laundering team with our colleagues in the NCA as part of the National Economic Crime Centre. We have a number of future campaigns, one around romance fraud, that we have had to defer because of Covid-19. There is definitely a move towards a more arrest-focused and pursue-focused outcome in terms of fraud.

Q705 **Tim Loughton:** I understand that. Everyone will appreciate the changing landscape, and there have been other priorities for all forces around CSE, domestic abuse and everything. However, your means of tackling this problem still leave a lot to be desired, particularly the efficacy of Action Fraud. Back in our report we said Action Fraud had irretrievably lost the confidence of the public. We see time and time again that there is still a problem in the clarity of the figures being reported to Action Fraud, and time and time again, as constituency MPs, we have constituents saying that they reported a serious fraud to the police, it just gets passed on to Action Fraud and they get a standard letter basically saying, "No further action is being taken." The figures for the success rate through Action Fraud have not improved. Is that not the case? Do you think that Action Fraud is the right way to be approaching this? Is it fit for purpose, or is it still as we discovered back in 2018?

Commander Baxter: The first thing I would say is that I believe a central place to report all fraud is exactly the way to go. HMICFRS supported that just over a year ago, and I think it is the way that we should manage how we report fraud.

I would say also that, since 2014, there has been a 41% increase in the numbers reporting fraud to Action Fraud. We have had a 41% increase in demand; we have not had a 41% increase in how we are funded. As of this year, there was a significant gap at the front end of how we fund Action Fraud. That said, Action Fraud is one part of a much broader system, and if we invest in the front end of Action Fraud, which I believe we should, we also need to invest significantly at a regional level and at a 43-force level. There are ways that we can do this, and I am sure Graeme will probably cover those, in our spending proposals and our fraud build across the system.

Q706 **Tim Loughton:** Mr Biggar, can you also build on your earlier point? I think you are saying that fraud is not taken seriously enough at whatever level, within the police or perhaps Government, or whatever; it ranks very low down behind other things that the Online Harms White Paper calls for.

Commander Baxter: I would say that fraud needs to be taken more seriously across all aspects of society. When we look at how people regard fraud, quite often I hear, "Oh, it is just vulnerable people who are subject to fraud." That is completely untrue. It cuts across all aspects of society. It cuts across media and it cuts across law enforcement. I think the issues and awareness around fraud need to increase significantly. We are working extremely hard to increase that awareness. We have had better coverage in our social media representation and education to people, and that is part of what we do in the National Economic Crime Centre as well.

Graeme Biggar: Action Fraud takes the heat from our collective inability to tackle fraud really effectively, but it is only one part of the system, and we need to fix the system as a whole if the whole thing is going to work. Action Fraud just collects the reports and passes them on. If there are not people who are able and willing to investigate them, the lived experience of your constituents will be the same, so we have to fix the system as a whole.

I completely support everything Karen said, but I would also say that neither of us is happy with where we are. We think we have made improvements over the last year, but we are passionately committed to doing an awful lot more and completely unsatisfied with where we are.

Your point about déjà vu is well made. Some of these problems are well known and have been around for a long time, and we need to fix them. We can do as much as we can with the resources that we have and with the systems that we have, which are changing, and we are really trying to step up our response to fraud. However, to get the step change we need, we need the five-point plan that we talked about before and the investment through the Spending Review.

Q707 **Tim Loughton:** Finally, I think you used the phrase that the taking down of sites is not as "slick" as it might be, and clearly Google are not taking this terribly seriously. They are not taking action seriously on something for which they are physically receiving money to prioritise on their

platform, or against some of the online harms where nasty individuals are posting hate, which is perhaps slightly more problematic in tracking down. They are profiting from fraud, and they are not responding proactively or favourably to your requests to be more active in not having it in the first place or to take it down straightaway when it is detected. Is that a true reflection?

Graeme Biggar: It is essentially correct. It is not a simple equation. They definitely take money to be pushed up the search results, and then there is a massive spectrum, from stuff that is completely legitimate to stuff that is very obviously fraudulent, with a lot of stuff in the grey area. It is around finding that grey area. At the moment the FCA would like it to be a lot more in the black and Google more in the white. We need to get the boundary shifted so that they take more off more quickly.

Of course, they are a worldwide organisation that have to deal with the legislation of lots of different countries, and that does present some challenges for them. That goes back again to the question Ms Abbott raised about us having better intelligence and understanding so that we can present that information to Google more effectively and make the case more compellingly. There is something for us to do there as well.

Q708 **Adam Holloway:** Commander Baxter, are there any ways of increasing revenues or any mechanisms that could be improved to send proceeds of crime towards the frontline or to penalise social media companies?

Commander Baxter: I believe there are ways that we can use what we call criminal money against the criminals themselves. One key area is the matter of suspended bank accounts. We have been working with UK Finance and a number of banks recently, who have, through much better processes, identified criminal money sitting in bank accounts that are highly suspected of belonging to criminals. In one bank alone I am aware of the sum of £40 million that is related to various criminal activities. Unfortunately, as it sits at the moment, that money will never go back out to victims and it will never be moved out of the bank because of the dormant accounts arrangement.

That bank has approached us, and we are looking at ways in which we can try to move that money or use it in a way that absolutely and directly benefits victims. There are difficulties with that. There are some legislative issues around money laundering, if the banks were to use that. I am sure my colleague Graeme will talk about some other work that is ongoing in terms of a judicial case to try to free up that money. There are definitely ways in which that can be used to benefit victims, and also to put barriers in and to investigate better the economic crime perpetrated by criminals.

Graeme Biggar: On the suspended accounts that Karen has talked about, we are working to free up the money that people think has been fraudulently received. Going to your slightly broader point, there is also the money that we recover from criminals and are recycling. Where there is not an obvious victim, we already have a system where a proportion or all

of the money that the police recover from criminals, depending on the means by which it has been received, can be retained and used to fight crime; not necessarily fraud, but crime generally.

Thirdly, and this is really worth mentioning, the Chancellor announced in the budget in March that he plans to introduce an economic crime levy, and there is going to be a consultation on that sometime this year, I think probably this summer. One of the questions that I expect will be asked, and I think will be worthy of this Committee's attention and of attention generally, is whether that money is restricted to being spent on money laundering or whether it is also spent on fraud. I think it would be very beneficial to ask generally if it could be expanded to allow money to be spent on fraud.

That will then be relevant to which companies or sectors it is levied on. There will be an argument that it should go broader than the traditional money laundering regulated sector of the banks, lawyers and accountants and into the other sectors or companies that fall into the "polluter pays" boundary of who might be relevant. That might bring in social media companies, for example. That is a really important opportunity for us generally to find a way of getting the right people to pay and of increasing the funding available to fight fraud.

Q709 **Adam Holloway:** One of you referred earlier to fraud being a public-private partnership. When I look back to when I was at *World in Action*, there were some amazing researchers there who seemed to be able to run down fraudsters as well as the best of the police. We have plenty of accountancy firms who do that sort of thing. Is there any way that you could bring people from outside the system on board, to incentivise people from outside the system to work with you?

Graeme Biggar: There is quite a big policy question there for Ministers about the extent to which that is the right thing to do. Whether private sector companies could be incentivised to recover the proceeds of crime and take a cut of it has been considered several times before. There is a more general point about how we can maximize the value from fraud investigators sitting in lots of different organisations around the country. There are more in the banks than there are, I expect, in law enforcement. I could not swear to that, but there are certainly a lot in the different banks, and in insurance and accountancy, too. There is something that we would like to do more of, and the Cabinet Office has led some good work on this already, to create a sense of a counter-fraud profession across the country, which encompasses private sector people as well as public sector people, so we can see it more as a collective endeavour.

Very specifically, and finally, Karen mentioned the fusion cell we are setting up. That is something we have been doing since the start of the year, although we have tailored it in recent months specifically to look at Covid. That has grand ambitions for the long term, but at the moment it is effectively a weekly meeting of law enforcement, regulators, the major banks and UK Finance, some insurance companies, some accountants and

Cifas. It is getting everyone together to try to understand what is happening so that they can spot cases coming through their books and refer them into law enforcement more slickly, and so that we can see the macro data coming out of that and spot the trends that otherwise we have not seen. It feels like the beginning of something really, really effective.

Q710 **Adam Holloway:** You say that the 46 forces around the country set their own budgets for fraud. Given that, certainly for online fraud, it is not happening or originating in their localities, is there an argument for bringing some of this cash—not all of it, of course, but some of it—more centrally?

Commander Baxter: You describe a really good point that is under significant discussion at the moment. If I go back to the figure that 86% of fraud has some aspect of cyber, the cyber network across policing is much more mature in terms of the investigative response. We have recognised across policing that there are benefits, probably, in bringing together cyber and economic crime investigations in a much more parallel and integrated fashion. That is under discussion at the moment. We have already worked with colleagues across cyber in terms of Operation Fortis, and that again is about cyber and how it impacts on small businesses, and then how we respond to that in policing.

There is certainly an alignment across policing that we believe needs to take place within the next two to three years. We are actively looking at that as we progress, and I have no doubt that Graeme will also mention that. It is not confined to policing; it is right across law enforcement and within banking. For example, when we work with our colleagues in banking, there is a similar process where cyber and economic crime information is being exchanged more now than it was, perhaps, 24 months ago, and it is where we need to take that in the next two years.

Graeme Biggar: There is also the question for the Government about how the 20,000 police officers that they have committed to being recruited are allocated, both to which organisations and to focus on which crime types. There is the strategic policing requirement that they can set, and the targets that they can put with it. One of the things I know they will be considering is the extent to which they make fraud part of that or, indeed, whether to allocate some of those police to regional centres to investigate fraud.

Q711 **Chair:** Thank you. I will ask some very quick, final clarifying questions. In our previous report we referred to an estimated 3% of reports to Action Fraud that ended up with a charge or a summons. Is that figure still the case?

Commander Baxter: I would have to check. I do not have that figure just off my notes at the moment. I do not want to give you an inaccurate figure. I might be able to get it before the end of the session. If not, I can supplement that afterwards. Sorry, I have just been given it here. It is 2%.

Q712 **Chair:** 2%? Okay, so it is even worse. What would a good figure look like?

Commander Baxter: I would look at anything around 30% or 40%. Ideally, what I would want is that every case of fraud has an outcome, that we are cutting fraud and protecting victims, and in an industrial way preventing fraud from happening.

It is not just about pursue; it is about, first of all, stopping victims being victims in the first place. The first thing is about industrialising how we prevent those crimes happening. The second thing is about absolutely changing how we in society, how we in policing and more broadly in law enforcement, deal with fraud, how we get upstream of it, how we disrupt and how we put barriers in place to stop the flow of money into criminals' pockets. Finally, it is about increasing the judicial outcomes for victims, and not just the judicial outcomes but also the repatriation of money back to victims from criminal accounts, which is particularly important.

Q713 **Chair:** I know, and we have heard a lot of those things. The big picture is that you have said an awful lot of things that all sound very, very good, but we are still on only 2%. That, frankly, feels shocking, and it feels like you need something much bigger and much more structural if we are to get anywhere near 30% from 2%. Do you not think that these five-point plans are tiny relative to the scale of the mountain you need to climb if you are to get anywhere near 30%?

Commander Baxter: The first thing is that the National Economic Crime Centre is just over a year old. In those 15 or 16 months we have worked extremely hard at putting together what we see as the best proposals that have ever been put before Government in terms of a whole-system build. You are asking me how we get to that. We get a whole-system build. It is much broader than policing, and it is a much broader thing than just law enforcement. It is about societal change, it is about banking and it is about the financial sector. That is critical if you want to move from a 2% clearance rate to something that actually makes a difference in people's lives. This will need investment.

Chair: Okay. Anything more you are able to send us in writing on the details of how we get from 2% to 30% would be very welcome. A very quick, final question from Diane Abbott.

Q714 **Ms Diane Abbott:** Commander, you said right at the beginning that you are basically a central reporting conduit, but you have almost none of the centrally held stats that we might expect you to have. My question is: to what extent do you think Action Fraud brings added value? Given that part of the problem, as you correctly said, is cuts in policing on the ground, might your budget not be better spent on paying for police officers on the ground to investigate these frauds rather than you being a central reporting conduit that does not seem to have many of the relevant stats?

Commander Baxter: We do have stats, and I can give you quite a number of stats. I can give you the number of frauds that are reported in terms of victim reporting. That is the difference. When we talk about fraud, it is

much broader than victim reporting. I can give you information around victim reporting, which I believe I have. I can give you information around the 822,000 cases that are reported by victims.

What I cannot give you is the information that sits in the financial system, in the banking system or in some other sector. That is why we need a full build, a much, much bigger build, way beyond policing. What I cannot give you all is what sits in my system or what sits in my colleague Graeme Biggar's system. We are working to bring those systems together to give a much better sense of the national strategic threat. That is the first point, and I think it is critically important. We have spent the last 12 to 15 months working together to put a plan in place to grow that. I think that is really important, and you are right about that.

The second thing is that there is the promise of 20,000 police officers, and we need to get those police officers into places like organised crime and, in particular, fraud and economic crime investigation.

The final thing I would say is that what we provide in Action Fraud is the equivalent of £24 million of call handling. When we take out the running costs, it saves policing in and around £12 million per annum. If we were to spend that £12 million elsewhere, we would have even fewer police officers to deal with fraud. Therefore, I think we provide value for service in a way that is very good, but we want to provide a better value for service and we want to provide better analytics and, most of all, a better service to victims.

Chair: Thank you. It would be very helpful to receive any further information you have on the way in which those figures are monitored when they go out to local forces, on what forces are doing with the cases that are reported to them and on what proportion of those get dealt with.

I thank you both, our first panel, for your evidence. That has been very helpful and very interesting.

Examination of witnesses

Witnesses: Susie Hargreaves and Robert Jones.

Q715 **Chair:** We are now going to move on to our second panel, where we are going to look particularly at some of the issues around online child abuse and online exploitation. Welcome to our second panel, Susie Hargreaves, the Chief Executive of the Internet Watch Foundation, and Robert Jones, the Director of Threat Leadership at the National Crime Agency. We have a series of questions for you, particularly on what the patterns have been around online abuse of children during the lockdown period and during the coronavirus period. I begin by going to Dehenna Davison.

Dehenna Davison: Thank you very much, Chair, and thank you to both our witnesses for taking the time to be with us today.

We know that, throughout the coronavirus pandemic, young people have

been spending a lot more time online. There have been some surveys that show that a lot of those young people are totally unmonitored. A survey by insurers Zurich found that one in 10 seven to 17-year-olds claim they were completely unmonitored during lockdown. We know that social media is one of those outlets that young people tend to use, but a lot of social media companies have been reporting that they have reduced their human moderation. Have you seen any direct consequences of that reduced human moderation?

Robert Jones: The answer to that is not yet, but I will explain the context, which is really important. The intelligence picture around the threat is that we identified very early, at the beginning of Covid, that paedophiles were seeing Covid as an opportunity to offend. We went public with that early, and we launched an education campaign where we went out and made that point. By now I would have expected more reporting to have come to industry around that element of the threat. In fact, across the world and from intelligence sources, there are indications that the threat has gone up and there has been more exploitation online, but we are yet to see that being reported through industry channels. The primary source for our insight into that level of offending will come from social media companies for a variety of reasons, which I can cover later in my evidence.

The important thing to recognise is that the threat is there, we articulated how we felt that threat would develop, and we took steps to educate people. There have been over 330,000 downloads of education materials designed to create resilience in children. What we are really worried about is that some of what has played out during the lockdown period will only manifest itself as lockdown is lifted. For instance, as children return to school, there will be another opportunity for them to engage with trusted individuals, with carers and teachers, and we would expect to see reporting develop from there on in.

Susie Hargreaves: Obviously, we were very concerned going into lockdown that more children were going to be online for a lot longer. The figures from the National Crime Agency are that about 300,000 people were potentially looking for child sexual abuse online. We felt there were an awful lot of worrying indicators. We are currently seeing a bit of a disconnect between the indicators and the actual evidence of an increase in online child sexual abuse. Placing that in context, a third of all the content that we removed in 2019—we removed 132,000 webpages—was self-generated content, and 80% of that was of girls aged 11 to 13. We were exceptionally worried about children being on their own in their bedrooms and potentially being open to the preying of perpetrators.

We have been working with the National Crime Agency, with law enforcement, with our partners and with industry to look at mapping what is happening and to come up with some actual evidence of what we are seeing. At the moment, we have this slight disconnect with indicators and evidence, but we are all working together. We need greater intelligence,

and we are all trying to ensure that, if we do see a massive increase, we are able to step up and take action accordingly.

Chair: Ms Hargreaves, we can only just hear you at our end in the Committee. Would you be able to speak a bit louder?

Q716 **Dehenna Davison:** Specifically on the point of moderation, do either of you have a preference over whether social media companies should be using human versus AI? It seems that social media companies tend to favour AI, but do you have a preference one way or the other?

Susie Hargreaves: At the start of lockdown, the IWF was designated key worker status, so we were able to continue to work in our office. We received a huge amount of support and help from the Home Office and law enforcement to enable us to do that, because we believe that we need human moderation. Of course, we are dealing with illegal content, so it is not something that people should be looking at at home.

The internet companies, across the whole internet, were also thrust into a series of firsts, where they were having to handle how they deal with moderation. They have some people working at work, some people working at home, but they have also had increased reliance on AI. That has raised a number of discussions and challenges that we are all talking about, which is, first of all, ensuring that people who are moderating at home have the proper welfare and the checks and balances, but also that the use of AI does not result in increased positives and negatives—that we are not getting false positives, false negatives and an increased amount of missed content.

That is a concern of ours. We still rely on human moderation for a lot of child sexual abuse, particularly in terms of children who are possibly 15 to 16, who would qualify in terms of child sexual abuse but might not be picked up by the AI. It is a concern, but I would also say it is a concern to industry as well. Last week we ran a roundtable on behalf of the Home Office with law enforcement and industry to try to bottom out some of these issues. What we are all aware of is that we need to ensure that we get the systems in place that work for the future. We want to ramp up AI, as long as it works, but at the same time we need to make sure protections are in place, because obviously they are looking at real children who have been sexually abused.

Robert Jones: Just to add a couple of points to that, I think AI is a really important part of the story. There is no way you can get across the volume on the internet without machine learning and AI. However, as Susie rightly points out, when you get into victim identification and age verification you need to be able to complement that with highly trained professionals who can assess those images.

During lockdown, one of the challenges that industry has had is how you tune that AI. What do I mean by that? There is a sweet spot where AI and machine learning will select images, and you can either, as Susie indicated,

over select or under select. You need human insight to be able to get that right. The challenge during lockdown has been either to set that AI in a way where it would effectively suppress reporting to prevent false positives and rely more on human moderation, or set it to the other side of that line, which could potentially generate more volume, more false positives and more noise in the system. Getting that right is really important, and that is where the number one eyeball from the people who have to do this terrible work and view these images is so important.

The answer is, yes, we need AI and, yes, we need machine learning. The future in terms of volumes and the way social media and the internet are developing mean we absolutely need it, but it does need to be tuned and complemented by professionals who can give you the insight to get it right.

That leads us on to the question of the lag in reporting, in that if there has been more use of AI and that has been very conservative, potentially as more human moderation comes back into the system on the west coast we could see more insight being generated and more reporting from the period of lockdown. That is one of the concerns that I have, that you have a bulge in the pipe in terms of demand that will only be released when human moderators begin to look at that product again.

Q717 **Dehenna Davison:** On the whole, would you say that you are content with the action that social media companies take to remove imagery?

Robert Jones: It is a really simple answer: no. We have given a lot of insight into the threat. We gave a lot of data, and we gave evidence at this Committee. We also provided evidence to the statutory public inquiry, and we made it very clear that we think the industry can do more.

There are some key areas where we need help because of the volumes. The first area is known images that are available on the internet. You will have seen volumes from the National Centre for Missing and Exploited Children being reported where there has been an increase in reporting from the US. A lot of that reporting is viral memes, which are known child abuse images that should not be shared—they are horrendous and they revictimise children—but people recirculate them out of moral outrage and in an attempt to get them taken down. That is part of the picture where we see availability and prevalence feeding the problem.

I can see no excuse, with the technology available to detect known hashed images, for that type of material to be circulating. While we pursue high-risk offenders, while Susie takes down websites, while we do all of this good work, we need demand taken out at the front end, and we need offending prevented. One of the ways you do that is by pursuing a very proactive and aggressive policy to take down known images. That is one of many areas where industry can do more.

Q718 **Dehenna Davison:** Why at the moment do social media companies not do this, or why are they reluctant to do this?

Robert Jones: There is a position in relation to the approach that social media companies, the ISPs and everybody in the tech world takes to this, and that has been built around an unregulated internet and around NGOs, people like the National Centre for Missing and Exploited Children, reporting on a very, very serious crime. This is articulated very well in the Online Harms White Paper, in the voluntary principles and in the findings from the independent inquiry into child sexual abuse. We find ourselves in a position where the response is being hampered by a lack of regulation. Much of this problem is extraterritorial. We are trying to influence, from the UK, tech companies elsewhere in the world to take this material down. The hosting figures in the UK are tiny, and Susie can talk you through that. The amount of material hosted in the UK is tiny. It is extraterritorial, and to extend our reach, to fight and to ensure that people who are truly responsible take this material down, things like the Online Harms White Paper become really important.

Susie Hargreaves: Obviously, I would like to reiterate much of what Rob said. In terms of your direct question, one of the things I wanted to mention was that the IWF's remit is dealing with content on the open internet and, in fact, less than 1% of what we removed last year was on social media. One of the things that is rarely represented is that, while the big household names are clearly dealing with the issue as well, there is a huge, complex internet infrastructure, most of which is hosted outside of the UK, where the companies who are hosting a lot of this material are names you will never have heard of. In fact, 90% of what we removed last year was on image hosting boards and in cyber lockers. It is absolutely essential that we take a look at the whole of the internet infrastructure and the whole of the ecosystem and, of course, within a global context to challenge and tackle this.

In relation to the social media companies, totally in relation to what we do, obviously they take our technical services and they work with us to disrupt the distribution. But as Rob says, there is clearly more we can do across the board, all of us working together to tackle this, to ensure that none of this content is uploaded in the first place.

Q719 **Tim Loughton:** I have to declare an interest at the outset as an IWF champion. Susie, can I come back to you? You published some figures recently that said that 71% of sex abuse images are hosted in the Netherlands, and some 90% of images are in Europe, whereas we tend to think of them as being from Russia, Alaska and far-flung, poorly regulated parts of the world, but they are not. Only a tiny part derives from the UK. Why is more action not happening in those democracies close to us to clamp down on this?

Susie Hargreaves: Yes, last year less than 1% was hosted in the UK. That has been consistent since 2006. That is testament to how we have worked together with law enforcement and industry in the UK. While we have an issue of people looking at content in the UK, we have a zero-tolerance approach to hosting it. We are able to issue a notice and takedown and

have it removed without going to court, and that is a fantastic position for us to be in as an organisation.

Take the Netherlands, which hosted 71% last year. That is over 90,000 webpages. There is a whole range of reasons why the content is hosted there. One is they have the internet infrastructure of hosting companies. They have a number of bulletproof hosts there who host quite dodgy material, and they do not have the legislation to remove it really quickly and effectively. We have been working with the Dutch hotline, with the Dutch police and with the Dutch Government via our UK partners, the Home Office and the police, to work collectively to get this removed. Clearly, if we could just stamp out the problem with the Netherlands, and if they could adopt a different approach, we would have a huge effect almost instantaneously. I think it is a question of them changing a whole ethos and approach to removing this content.

Q720 **Tim Loughton:** So, we are ahead of the game in many respects in what the IWF is doing, and it would be good if that was replicated in many other countries. We are still waiting for the online harms code. How important is that as a further weapon in the armoury, and how important is it to get that sooner rather than later? The Government have promised it, but we still have not seen it.

Susie Hargreaves: I totally echo what Rob has said, that we desperately need the online harms legislation speeding up. We need to know where we stand. The level of uncertainty is really unhelpful to us all. We are still waiting for the online harms formal response and the code of practice, and all of us collectively need to know what is going to be within the scope of regulation and what we are going to be required to do. It feels like we are all operating in an unclear space at the moment. That is across the board; industry, law enforcement and ourselves are all pushing for that.

How will it help internationally? It will obviously have to take into account other legislation outside of the UK, but I think the rest of the world is looking to us in relation to our regulation and what we are doing to find ways to mirror it and learn from it. Certainly, in relation to the Netherlands, any pressure that can be brought to bear from the UK Government and from parliamentarians is hugely gratefully received because it is a major problem. Having said that, in the last year they have really started to engage with the issue.

Q721 **Tim Loughton:** Robert, by all means comment on that, but could I just turn to the NCA's strategic assessment? It is estimated that there is something like 300,000 individuals in the UK who pose a sexual threat to children, either by contact or online abuse. How do you come up with a figure like that—it seems a large figure—and how do you keep track of them?

Robert Jones: I will cover the online harms element briefly, then I will come on to the scale of the threat.

On the issue around regulation and progress, from an NCA perspective we worked hard to provide evidence to the independent public inquiry and policy officials in relation to that proposed legislation. There are some key areas that are of particular interest to us in terms of sanctions and our ability to make this matter in terms of the future. One of those is the ability to potentially block, through ISPs, platforms that are not compliant. I give that as an example because one of the things we must have is the ability to make a difference as this progresses because, as I have pointed out, the problem is extraterritorial with a lot of the hosting, so from the UK we need to be able to project that response.

Moving on to the point about the scale of the threat and the 300,000 figure, that is an assessed intelligence picture. It is not an exact number; it is based on our assessment of a range of different sources of intelligence, which we keep updated. Now, we have growing insight into activity on the dark web, and sadistic forums on the dark web that are entirely devoted to child abuse. They are advocates for child abuse, they publish paedophile manuals, they incite abuse and incite the generation of images. Through some of our intelligence activity we have growing insight into volumes on the dark web. Without going into the detail of those tactics, we are confident that there are thousands of individuals who are visiting those sites from the UK.

If you then look at the individuals who have been caught and are the subject of management through the MAPPA process and the sex offenders register, there is another cohort of over 25,000 individuals who definitely have a sexual interest in children. Then if you look at the data around people attempting to access child abuse images, which is in the millions, and the level of referrals that we get from the National Centre for Missing and Exploited Children, you get a number of building blocks in the intelligence picture that drives you to that figure.

That figure in itself, when you reach that scale of threat, it is self-evident that we need to do more than just arrest people to mitigate that threat. To your point about what we do about that, part of the response we have just touched on is that we need offending to be prevented and we need demand to be reduced through preventing access to known images on the internet. Our big concern is that that is feeding the problem. There is a demand reduction and prevention element to this that is really important. We contribute to that through insight in relation to education and creating resilience in children and allowing professionals to understand through our work in CEOP exactly what offenders are like.

Then there is the hard-edged pursue element, which is arresting perpetrators. With Simon Bailey, who is the lead for national policing, we have a large-scale response to arresting these individuals, where we are chasing every intelligence lead that we receive from the US and every intelligence lead we generate ourselves. That manifests itself in approximately 700 arrests every month and 600 children being

safeguarded. Last year in the region of 7,212 individuals were arrested as a result of that joint activity with national policing.

So, as you can see, that pursue machine, looking at volume of offending, is running very hot and we are arresting and pouring into the prison system literally thousands of offenders.

Q722 **Tim Loughton:** Which is very encouraging to hear. We visited NCA and saw some of the gruesome things that your officers have to trawl through. I think Simon Bailey has done a fantastic job as the lead chief constable on this. I remember having a discussion with him in the media a while ago where he was making a case for not taking action against some of the lower level offenders who have accessed abusive images, where they will only get a warning. I took issue with that on the basis that we know it is a gateway to more serious abuse. At the other side of any abusive image is a child who has been abused in order to produce those images.

Do you think that we could or should be targeting more people at an early stage to try to prevent them from becoming more hardcore accessors of abuse? Are we targeting the right people, or is it just down to a resource issue?

Robert Jones: There are probably three things I would like to mention. The first thing is that we need to raise the entry level for offending in this space. This is absolutely about the open web. Nobody goes straight on to the dark web to start looking at child abuse images; they start on the open web. The barrier for entry to this type of offending is simply too low. We should be taking early action on people's browsing habits, and the Lucy Faithfull Foundation and others describe this very eloquently in what they see when people ring for help. People are becoming desensitised by accessing extreme pornography, more and more extreme material online, which is really easy for people to identify and download.

They then start a journey where they will meet like-minded individuals, who will tell them that that is right, and they will normalise that behaviour, which is not normal and is a threat to children. Once they take the next step in that journey, they may end up on the dark web where they will be directly incited to produce new images of abuse, which creates a direct causal link to contact abuse. So, point 1, raise the bar, stop people accessing the material. There is nothing good about people seeing this. It is not about freedom of expression. It is plain wrong. Get it off the internet.

Step 2 is when people start to engage in risky behaviour and they may not yet have offended. Early intervention in that space, at scale, is an absolute opportunity to reduce offending. Once people offend, it is absolutely our job from a law enforcement perspective to pursue those individuals and that is what we are trying to do. The scale, the amount of arrests and the size of the system in the UK speak for themselves. We will continue to pursue those offenders, but concurrently we need industry and we need greater input at the start of that offending journey to take people out of the game and reduce demand.

Tim Loughton: That is very clear, thank you.

Q723 **Andrew Gwynne:** Just to rewind a bit, clearly there have been fears that online abuse of children could increase during the lockdown period. Accepting what you said to my colleague about the lag in reporting, Europol, the Internet Watch Foundation and, in written evidence to this Committee, the NSPCC have all said that there are early signs of increased demand for child sex abuse imagery. Very quickly from you both, do you accept these assessments?

Susie Hargreaves: Yes, we published some data that we had from three major companies about hits against our IWF blocking list during April. We recorded 8.8 million attempts to access the list. There is no data from another period outside of lockdown to compare that to but, even so, it was quite worrying data in terms of the numbers. Our feeling, based on our experiences, is that there is often a time lag between images being taken and then making their way to being circulated on the internet. If you look at the overall trajectory, particularly in self-generated content, we are expecting to see more of that content start to show over the next few months.

Yes, we are concerned that we will see an increase, but we also need to ensure that we talk to companies and that we take on board if they are seeing evidence of more reports at their end as well. The conversations we are having at the moment are that we are all worried, we see these indications and we have this sense that we are going to see a big increase, but we need to counter it, balance it and make sure that we are looking at it against the actual evidence. We are all measuring at the moment, and I think the important thing is that we are ready if we do see a massive increase come back into the system.

Robert Jones: I have a couple of points. In terms of professional judgment, yes, I do recognise what is being reported. I am concerned. I am particularly concerned if people have been locked down with abusers. This by its very nature is a hidden crime. A lot of image production is connected to familial abuse, let's not forget that. A lot of the victims referred have been abused by people in positions of trust or other family members. For that to filter through and get to us, children need access to a trusted channel of communication to do that.

As children return to school, I think we will see more of that. As lockdown eases, I think we will see more of that. We have done everything we can, including meeting high-risk offenders head on during the lockdown period. We have done 50 search warrants in the NCA alone since the lockdown, 52 arrests. We have really gone for the people we are worried about to try to push and pull through the intelligence around abuse during lockdown.

To summarise, everybody that is reporting internationally is reporting a concern that more has gone on. We need to be ahead of that, and national policing, through Simon Bailey's public protection portfolio, with policy officials have made this point in terms of local safeguarding arrangements.

That has been made quite early to ensure that people are ahead of the problem and waiting if it does peak but, crucially, are being proactive during lockdown to try to communicate with potential victims.

Susie Hargreaves: During the lockdown process there have been a number of meetings and get-togethers to share what we are finding. The UKCIS, the UK Council for Internet Safety, early warning group is meeting with all the NGOs, law enforcement and people who run help lines and hotlines to share what we are finding. We have been meeting with industry to share what they are seeing, and Simon Bailey runs a fortnightly meeting sharing what is happening from the law enforcement side. We have got to a point where we are all needing to collate and collect that information in a meaningful way.

Q724 **Andrew Gwynne:** Is that something you would be able to share with the Committee at the appropriate stage when you have a clearer picture of what is going on?

Susie Hargreaves: Yes, I am sure. As actual hard data starts to emerge, we will be able to start collecting that information and share it with the Committee. I don't have anything specific to share at this time.

Q725 **Andrew Gwynne:** No, I appreciate that. Moving on to enforcement, and perhaps to Rob Jones, in the year ending September 2019 there were, on average, 450 arrests for child sexual exploitation and abuse and, I think, 600 children safeguarded each month in the UK. What is your assessment of the specific impact the Covid-19 crisis and the lockdown has had on this?

Robert Jones: We have managed to sustain, with national policing, the volume response. The figures during the lockdown for pursuing referrals from the National Centre for Missing and Exploited Children, for instance, have remained in the same general area that they were before lockdown. Those referrals are still going out to policing, so there has been over 3,200 referrals to local policing during that period. They are out on the ground making arrests, just as we are. We continue to perform at that level. The NCA has pivoted towards high-risk offenders who are operating on the dark web internationally and the pillars of threat and demand that are harder to tackle, which we are really built to tackle with the type of capability we have. Meanwhile, we are concurrently working with industry to provide them with insight and also with national policing to keep that volume moving.

The answer is that we have sustained the response for what we have seen reported, and we have proactively sought intelligence to try to bridge the gap between our professional judgment that there will be more abuse and what we are actually seeing reported from industry. As Susie has pointed out, all of the combat indicators are upwards with a trajectory of threat that looks like it is going up. What we are not yet seeing filtering through is the referrals from industry that match that. We have not waited for that; we have been proactive with our intelligence work to try to get in among it and disrupt that threat during the lockdown period.

Q726 **Andrew Gwynne:** I am interested in the views of you both on the Government's response to the threat of online child abuse during the pandemic. In addition to moving faster on online harm legislation, which Susie mentioned a moment ago, is there anything else that you would have liked to have seen done by the Government in this area?

Susie Hargreaves: We have been very heartened by the Government's response to the pandemic and certainly how it has affected us. As I say, we have had constant engagement with officials and Ministers during the period, and we are currently in discussion with the Government about awareness raising, particularly for young people and carers, on the issue of self-generated content, because we need to get some very clear messaging out to get children to keep themselves safe. We need to get that finalised, and that is the area where we think we need more support. Overall, we have been extremely heartened by the Government's response during lockdown.

Robert Jones: It is a similar experience. We have a Home Secretary who is seized by the threat, and the previous Home Secretary was. We have had strong support. Our daily briefing battle rhythm has fed into the understanding of officials and Ministers in relation to the threat. We have taken part in roundtables and, as Susie has pointed out, discussions with industry to try to make sure that some of the barriers to communication are broken down. On balance, we have received a great deal of support, and we have been able to make our case and our concerns heard.

Q727 **Andrew Gwynne:** Finally, I just want to touch on something that came up at an earlier session. The Home Office Minister, Baroness Williams, in an evidence session a few weeks ago, called Facebook's plan to introduce end-to-end encryption on its Messenger service a very worrying development. How much of a concern are private communication channels, and what can be done to address illegal imagery or activity on these private forums?

Robert Jones: I am deeply concerned about the Facebook proposals. We have articulated those concerns to Facebook through policy officials and directly with them through bilateral meetings. In essence, the system that industry run at the moment relies on them being able to inspect their own traffic. Their internet traffic is unencrypted in its current form, and they are able to detect known images, they are able to detect grooming and they are able to detect a number of indicators for those, which are reported through the NCMEC. What Facebook has been unable to explain is how, when you apply the end-to-end encryption model and you lose that insight and ability to look at hash values, text and all of those things, they will replace that with a regime that does not effectively turn the lights out for law enforcement and prevent us from getting that insight.

We cannot unknow what we know. We know that Facebook features in many of the grooming cases, and we have shared that with them. We understand how offenders behave and target vulnerability. Offenders will look at things like Facebook, WhatsApp, anything with an end-to-end

model, and will realise very, very quickly that there is now less ability to inspect material on that platform. They are very clever, they are very cynical, they exchange tradecraft on the dark web, and this will be a topic of conversation for them. We are deeply concerned. We have articulated why in an evidence-based way, and I am worried for the future.

Q728 **Andrew Gwynne:** How receptive has Facebook been?

Robert Jones: From my perspective, the law enforcement liaison people we deal with are absolutely committed to child protection. If we give them a lawful order in the UK, they will assist us in any way they can. If we work through the UK/US agreements in the future, again they will help us. But it is not those individuals who concern me. I cannot get to the Facebook board to make my case. I would like to see the person who does risk on that board and the person who is responsible for their finance to be absolutely gripped by this. I don't know whether they are, because I do not see anything publicly that describes their position in terms of mitigating that risk.

Andrew Gwynne: That is a big worry.

Susie Hargreaves: To echo Rob's concerns, we work very closely with Facebook, who take a number of our services, to disrupt the distribution of child sexual abuse, and they also support us in many other ways. But we are also very, very concerned about the intention to encrypt Messenger and the impact that will have on victims of online child sexual abuse. We are calling for equivalency. Basically, we are asking Facebook to give assurances that child protection will not be hampered and that children and victims will be protected in some way. As yet, none of us has seen any of those assurances. Across the whole child protection sphere, we are all concerned about the encryption of Messenger.

Andrew Gwynne: That is very worrying. Thank you.

Q729 **Chair:** Just to follow up on that, in addition to that your clear concern about Facebook and social media, if you are looking forward over the next 12 months, two to three years, what would be your greatest concerns or the issues that you would flag up as potential future risks?

Robert Jones: There are a number of things. First of all, the prevalence of end-to-end encryption is a real threat to our response. That is well rehearsed and we have explained why. The second point is on the open web where there is a really low barrier to offending. There was a time when the online abuse picture shone a light on a problem that had been hidden. That time has passed, and now it is feeding the problem and creating more offenders.

We have seen an exponential rise in online abuse over the last 10 years. In the next 10 years we will see the same demand curve unless something happens now to raise the bar and stop people getting involved in this horrendous behaviour. That hard stop to take demand out of the system needs to happen now because, combined with encryption, increased

internet use, 4G and 5G are being rolled out to Africa and developing countries. We describe our response to child abuse where we chase every offender. Go to Africa and look at the response in many African countries, because they are unable to tackle the scale of the threat. Deliver that technology in those environments and you will again see an exponential rise in online abuse. The proportionate response to technology improvements needs to come, and it can only come through more responsibility from technology companies.

Susie Hargreaves: We would also like to see a number of things over the next two to three years. We are concerned that the regulation is clear, adds to what we have already been able to achieve in the UK and makes us more effective. We want good regulation and we want it soon, and we want legislation soon that helps us remove this uncertainty. We also want a stronger focus on education and awareness.

While there is a huge amount that tech companies can do to stop the proliferation of these images, there is also the education piece. We know that young men aged 16 to 25 are extremely vulnerable to start viewing online child sexual abuse, so we need to tackle the whole prevent and behaviour side as well as using technological solutions. We are really concerned that everybody thinks there is a magic bullet solution that can be done by the tech companies that will resolve the problem completely. We actually need to approach it from three angles, from a legislative angle, from an education and awareness angle, and then also from a technological angle. We need to get more messaging out about a zero-tolerance approach to child sexual abuse.

We also need to think about the funding for this. For the IWF, 10% of our funding comes from the EU. There are no assurances yet that the Government will be able to pick that up, which impacts on the UK Safer Internet Centre.

Q730 **Chair:** Can you just clarify that funding issue? Is it a significant shortfall?

Susie Hargreaves: It is. For the IWF it is 10%, which is about £400,000. For our partners, South West Grid and Childnet, it makes up to 50% of their funding. Without that money, Safer Internet Day will not run. This year Safer Internet Day reached 50% of all children in the UK, so it is absolutely essential that we have some assurances in place that the UK Safer Internet Centre will be protected after the European funding ends.

The other thing I wanted to say is that obviously one of the key problems and concerns we have is not just about the changing nature of the abuse—we all need to step up and fight that in whatever way we can—but we are dealing with a global issue. As Rob says, we have an issue where people in Africa are going straight on to 4G and 5G, so the access to child sexual abuse is instant, yet we need to ensure that we have mechanisms and legislation that enables us to operate effectively internationally.

Q731 **Adam Holloway:** Some time ago one of my team sent an e-mail from her

parliamentary account and it was flagged as being pornographic. It turned out the e-mail was a photograph she was sending to her dentist. If systems can do that, and if systems can do facial recognition to recognise whether it is a child or an adult, is it beyond the technical bounds of possibility to be able to electronically identify pornographic images of children?

Robert Jones: It is absolutely possible. One of the IICSA recommendations is that tech companies prescreen and prefilter their traffic. What does that mean? That means that, before material is available on a server where other users can share it, they identify during the upload process the type of material that you are referring to. That is doable; it is doable now. It is used to defeat intellectual property violations. It is used in a range of different ways. Scaling up that use would allow, just as the IWF does, an approach that blocks and prevents offending rather than what we currently have, which is a regime where the offending happens and it is reported after it has happened. Yes, it is possible.

Susie Hargreaves: Yes, I agree it is possible. We are all using increased AI and machine learning, so one of the things we are able to do now is that we hash known images, which means we are able to go out and search for duplicates. These tools really help us fight the problem. The AI and machine learning is getting better and better at judging a child's age, but there is still no technology in the world that is absolutely 100% able to age whether a child is 15 or whether it is an 18-year-old adult. We still need human assessment in order to ensure that we are removing content that is illegal.

Chair: Thank you very much. I thank the panel for the evidence that they have given us. We will certainly pursue further some of the issues that you have raised, including some of the issues that you have raised about Facebook.

Finally, before we conclude this session today, while we have been in our evidence session the National Police Chiefs Council has made a statement on behalf of police forces across the country on the awful murder of George Floyd in Minnesota. It says, "We stand alongside all those across the globe who are appalled and horrified by the way that George Floyd lost his life. Justice and accountability should follow." It also refers to the UK tradition of policing by consent and the need always to tackle bias, racism and discrimination wherever we find it.

I want to welcome those words because this murder has appalled people right across the world, and so too have some of the violent responses from US police officers towards peaceful protesters and journalists. Some of those disturbing scenes should, I think, instil in all of us the need to redouble our commitment to tackling racism and injustice wherever we find it.

Our Select Committee, before the election, had begun an inquiry, two decades on from the Macpherson report into the racist murder of Stephen Lawrence, to look at race and policing in the UK today. The Committee is continuing with that work. Last week, when reports emerged that the fines in the coronavirus regulations had potentially had a disproportionate

impact on those who are black or ethnic minority, I contacted the NPCC to ask them to provide us with detailed information, force by force, on those fines by ethnicity. We would expect to publish that information when we have it and also to take further evidence from the police, which we will be doing, on that issue.

Our inquiry is continuing, so if people have further information or reforms that they want to put to us, we will welcome that as well. As Government Ministers, Opposition leaders and people from across the parties have made clear in this country, it is a responsibility on all of us to show our sense of solidarity and to be very clear that black lives matter. We should challenge racism wherever we find it. Thank you very much.