Select Committee on Communications

Corrected oral evidence:
The Internet: to regulate or not to regulate?

Tuesday 15 May 2018

3.30 pm

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall.

Evidence Session No. 5 Heard in Public Questions 35 - 43

Witnesses

I: Ms Susie Hargreaves OBE, Chief Executive Officer, Internet Watch Foundation; Chief Constable Stephen Kavanagh, National Police Chiefs' Council; Mr Will Kerr, Director of Vulnerabilities, National Crime Agency; Mr Donald Toon, Director of Prosperity, National Crime Agency; Detective Superintendent Phil Tomlinson, Head of National Digital Exploitation Service, Metropolitan Police.

Examination of witnesses

Ms Susie Hargreaves, Chief Constable Stephen Kavanagh, Mr Will Kerr, Mr Donald Toon and Detective Superintendent Phil Tomlinson.

Q35 **The Chairman:** I welcome the witnesses to our session on regulation of the internet. Our witnesses are from the Internet Watch Foundation and law enforcement agencies. The meeting will be broadcast online and a transcript will be taken.

Our inquiry is seeking to establish whether or not we need to regulate the internet further. While exploring that, we are very keen to look at the balance between further regulation and freedom of expression.

Will our witnesses briefly introduce themselves and tell us a bit about their background and the organisation they represent? Perhaps in your opening remarks you would tell us the main challenges that you face in dealing with internet crime, and whether the legal powers that you enjoy are adequate to face up to those challenges.

Ms Susie Hargreaves: Thank you for inviting me to speak. The IWF is the UK hotline for reporting and removing online child sexual abuse. We operate in a trusted triangle between law enforcement and the internet industry. It is a very delicate balance. Our plea is that our self-regulatory approach is acknowledged as working, as we believe it is the best way to remove online child sexual abuse; it is a model that is not broken and does not need fixing.

We are one of the most successful hotlines in the world, with an unrivalled track record for speed of removal of content, which in the UK is typically less than two hours. The UK has gone from hosting 18% of all child sexual abuse to less than 1%. The UK is one of the most hostile territories in the world for hosting online child sexual abuse. Ninety per cent of our funding comes from the internet industry and 10% from the EU.

To give you a sense of the scale of the problem, child sexual abuse is not something that we think will be solved. It is a war of attrition and we need to keep fighting to attack the crime. Last year, we removed 78,500 individual web pages of child sexual abuse, of which 90% were girls and 55% children under 10. We are talking a lot about babies who are raped and tortured. Over the last three years, 65% of the content we have removed of children aged nought to two was category A, which is rape and sexual torture.

As an example of what it means for survivors and victims, last year I met a very brave 18 year-old woman in the States. In the States, you can opt to be notified if anyone is caught with a series of your images. She was rescued when she was 12, after 12 years of appalling abuse. Her father received 60 years in prison. She had already received 1,500 notifications from US law enforcement of people being caught with her images. One of the images had been shared more than 70,000 times. Appallingly, when she was 13, a man came up to her in a supermarket and talked about

seeing her images online. These are real abuse victims, and every time someone looks at that abuse the child is revictimised.

In relation to the challenges and the legal position, our model of self-regulation works and goes right to the heart of the questions posed by this inquiry. We believe there are lessons learned from the 22 years we have been in existence that we can share. We are dealing with the very worst of the internet, which we call the internet sewerage system. No other form of content online has been as successfully removed as child sexual abuse under the self-regulatory model we apply, because the definitions of child sexual abuse are widely accepted in the UK and internationally, and our assessment is clarified in UK law. Very importantly, unlike other internet harms, we do not have to go before a judge and jury for someone to take an opinion, and we can act quickly to have the content removed.

The challenges for us are threefold. The first challenges are technical. Technical solutions alone will not resolve the issue. It is important to work with the internet industry. Secondly, it is important to understand that there are social and educational issues about raising awareness of the crime. The third challenge is on the regulatory front. We believe we have the necessary laws and legislation in place to be able to act and that we are in a very privileged position to do so, but it is not a model that particularly works elsewhere in relation to other types of content.

To finish, I reiterate that we have a very delicate triangle of trust between law enforcement, the internet industry and ourselves, and we have a model that works exceptionally well. It's not broke, so please don't fix it.

Chief Constable Stephen Kavanagh: I am currently chief constable of Essex. I am also the lead for the National Police Chiefs' Council for the digital policing portfolio. That is divided into three areas: how the public can contact policing in the digital age, moving on from the 999 system; how we can use that information more effectively to analyse, develop intelligence and investigate, which is to do with the skills of the officers involved; and how we can consistently present that data in the criminal justice system.

I have come straight from a digital policing board that I chaired this morning. Things are progressing in an encouraging way as regards police chiefs taking responsibility. I have been a police chief constable for five years. When I first became a chief constable, I was at a regional meeting where one of the chiefs said, "We don't have a digital policing problem". That was an enormous concern, because some chiefs did not even know what they did not know. There is now an ambition for us to try to make sure that we can work with other stakeholders to understand where those harms are taking place.

My experience as ex-commander of counterterrorism at Scotland Yard and deputy assistant commissioner for specialist operations is that a two-tier level of capabilities had been developing. The security services,

counterterrorism teams and the National Crime Agency have developed a very high level of capability and very good relationships with some of the internet providers and other developers.

My concern was about mainstream policing. Where were local forces organising themselves? What was going to happen to a victim of abuse online, to someone who was harassed online and to the victim of fraud or anything else that was taking place? How could we ensure that policing was more consistent in the way it responded to victims? The 1950s "Dixon of Dock Green" model of policing is a bygone concept. Of course, we need bobbies in communities; that is part of what we must be, but we must also be fleet of foot and understand the legislation.

I have a slight concern. Some of the top-level crime sites are taken down quickly by providers. There is the capability to remove sites quite quickly when the need arises, but a lot of things are still going on both on the open web and on the dark web. Enabling legislation, with appropriate judicial oversight, can help us to go more quickly after the sites and to where the funding opportunities might be for criminal endeavours.

As to where the 43 chiefs are, the days of people saying that we do things 43 different ways are no longer true. We are increasingly consistent in the way we develop capabilities. There is an ambition within policing to be better, but also enough humility for us to say that there is an enormously long way to go to develop skills, and understand what you do at a burglary scene when a digital footprint is there but DNA and fingerprints are not. I am here both to explain where we are progressing well and to show humility about the ambition of mainstream policing to try to improve in this area.

The Chairman: You touched on a number of the issues that we want to explore today, and that is a very useful introduction.

Mr Will Kerr: I am director of vulnerabilities for the National Crime Agency. To give you a sense of the NCA's statutory responsibilities, by law it is responsible for leading the UK's fight against serious and organised crime. Steve touched on some of those responsibilities. Within the NCA my portfolio includes CSEA, which is child sexual exploitation and abuse; responsibility for CEOP, the Child Exploitation and Online Protection Centre; and organised immigration crime, modern slavery and human trafficking. Of relevance to your hearing today is that social media are being used to facilitate the criminal exploitation of vulnerable people in all three of those threat areas. Increasingly, social media are used to recruit and trade vulnerable people. This is now a global phenomenon; it is by no means restricted to western Europe or the United Kingdom.

I will take a slightly different approach to the CSEA thread, if I might touch on that briefly as a practical illustration. I think the system is broken and fundamentally needs to change, and there are simple things, particularly in our relationship with industry, that can happen to help protect thousands of young children across the United Kingdom today and tomorrow from the risk of child sexual exploitation and abuse.

I am happy to go into more detail later, but, briefly, the scale and nature of the CSEA threat has changed fundamentally over the course of the last five years. The scale has risen exponentially to the point where the law enforcement system is struggling to keep up with it. If we take industry referrals alone, we get most of them through a charity called NCMEC, which is the National Center for Missing and Exploited Children. It is housed in north America because that is where most of the big companies are based.

The number of referrals that the NCA has had since it was created in 2013 has risen 700%. That has stretched the capacity of the law enforcement system in the United Kingdom to keep up. The scale has fundamentally changed as well. All CSEA is serious. This is not about grading its seriousness, but we do need to grade its risk. The exponential rise in volume has masked the risk factors that have developed and evolved over the course of the last number of years. Live-streaming is an example.

The IWF published an impactful report today about live-streaming, but we are now dealing with organised crime gangs in Thailand, the Philippines and the Far East that are motivated not by sexual predilection but by the need to make money. A number of organised crime gangs in those countries are now engaged in the live-streaming of content abuse to order. A paedophile sitting in the United Kingdom willing to pay for this service can designate the ethnicity, age and dress of the child they want to see being abused, and they can direct that abuse online in live time. That is a fundamentally different type of risk from the one we faced before. It is one we should be deeply concerned about, and we need to think of more innovative, original and disruptive ways to stop that type of offending.

You asked about legal powers. I would be more than happy to come to that later. I am conscious that you want reasonably pithy comments to start us off. Of course, being pithy does not come naturally to the Irish.

The industry could do a number of simple things, but we need fundamentally to reset our definition of success in protecting vulnerable children, so that we are not looking at definitions of success based on finding and reporting more offending to the criminal justice system and prosecuting more offenders. As an institutionalised cop, I am always happy to take more people to court, but we should be defining success as our ability to prevent offending in the first place, with the same technology that is being used by offenders to target, groom and abuse our children, and stop thousands of kids becoming unnecessarily subject to that vile abuse. I will end on that point. I am more than happy to go into detail on any of those points later.

The Chairman: Thank you for your vital work in this critical area.

Mr Donald Toon: I am the director in the National Crime Agency responsible for economic crime and cybercrime. There are two direct links to some of the issues that the Committee wants to cover.

I want to pick up the previous comments on internet content. One of the fundamental issues from my perspective is the use of online capability as a specific tool to target UK businesses, individuals and the public sector, either to damage their ability to operate, or to make money by locking organisations out of their data using ransomware capability or by using online currencies to carry out a form of extortion directly online.

A range of issues are specifically important from a UK perspective. One of them, which Steve Kavanagh alluded to, is the break in the direct geographical relationship between the criminal and the victim. It is fundamentally a worldwide problem. Secondly, from the cybercrime perspective, there is the difficulty of cross-over between activity that is purely criminal in nature and activity that has a hostile state relationship. That is a real piece of complexity. Thirdly, that capability can become a set of commodified tools available for purchase using the dark web. People are able to develop a capability, using tools being created by top-level criminality, to carry out a series of attacks anywhere in the world and at any point in the UK. Those are some fundamental issues for us.

You asked earlier about whether the system is broken. From a cybercrime perspective, it is not that the system is broken but that it is developing. The system is trying to develop to catch up with a very fast-moving and fast-developing criminal threat. We have seen that in the scale and growth of cyberattacks and cyber incidents over the last three years. From a UK perspective, that was probably highlighted in the UK by the WannaCry attack that affected the NHS last year.

We have a very effective, strong relationship with the National Cyber Crime Unit in the NCA working very closely with regional organised crime units, and developing capability within forces to tackle cybercrime. That has to be seen in the very close partnership with the National Cyber Security Centre. Fundamentally, we have an opportunity to do some strong law enforcement activity, but there is a protection and prevention issue, which, given the worldwide nature of the criminality, is absolutely critical to our way forward. How do we use effective partnerships with major corporate operators to ensure that prevention and protection are effective?

Detective Superintendent Phil Tomlinson: I am the outgoing head of the National Digital Exploitation Service for counterterrorism policing. We provide a number of dedicated capabilities for the counterterrorism command in London, a number of support functions for wider counterterrorism policing in the UK and some support functions internationally.

We provide seven services for counterterrorism policing. There is communications data exploitation, which is the recovery of data that companies collect about individuals' account histories, cell site data, billing information and so on, which we use UK legislation to obtain. We have the open source exploitation service, which incorporates the Counter Terrorism Internet Referral Unit, which you may have heard of. It engages in the takedown of terrorist content. I am sure we will talk

about that this afternoon. Since the creation of that team, we have withdrawn more than 300,000 videos, documents and speeches from the internet by working with industry, obviously collaborating very closely with our colleagues in wider policing.

The next service we provide is to do with digital media exploitation, which is conventional digital forensics. We are one of the UK's lawful intercept agencies. We provide a technical innovation and development service that develops new software and works on decryption and advanced forensic recovery from recovered devices and so on. We have a digital biometric service that is developing new capabilities for the collection of biometrics, and increasingly using biometrics to access data. You will know from your own devices that a lot of data is no longer obtained through passwords and passcodes; it is now accessed through biometrics, so we are looking to understand that technology and apply it in terrorist investigations in the UK. Lastly, there are digital operations, which provide a lot of multisource analytics, understanding data, contextualising it and, more importantly, presenting it so that people can understand what the data means, not just for investigations but for prosecutors, courts and ultimately members of the public in their role on juries in public prosecutions.

The first big challenge for counterterrorism policing is the volume of data we collect in investigations. A typical terrorist investigation will recover approximately 10 terabytes of data. Some of the big investigations can involve between 30 and 50 terabytes. To put that into context, if you were to print it out on A4 paper, the pile would be about 100 miles high. Unfortunately, with those increasing volumes of data we do not have increasing numbers of police officers to deal with it, so we are looking for multiple pins in multiple haystacks stored in multiple parts of the world, and we need to try to piece that information together and understand it so that we can look for the evidence when we may have people in custody.

The next big challenge for us is around the encryption of data. If we are able to obtain data, we need to understand it and decrypt it. Often, the encryption changes very rapidly. Some of the bigger companies might change their encryption twice a day, which means that, if we are able to obtain information on a Monday morning, by Tuesday morning we will have to come up with a new solution to obtain the data. That is an increasing problem for us and probably takes up most of our time.

The next challenge, which I think we will talk more about this afternoon, is around social media. Social media have presented three big issues for counterterrorism policing. The first is ease of access to information about terrorist groups. In the last few years, we have seen vulnerable young people finding information online that provides advice and guidance about how to travel to foreign countries to engage in terrorist activity.

Secondly, it is very easy for individuals operating in terrorist groups to put their messages out. We have seen propaganda, beheading videos and the like broadcast on the internet in recent years. Thirdly, there is the

ease of direct communication between individuals and terrorist groups. A large number of the social media companies provide messaging services. I am sure you use some of them yourselves when communicating with friends. People often ask us how terrorists communicate with one another. It is exactly the same way as we all communicate. Technology has advanced to a stage where we can communicate securely and safely, and there is no need to engage in particular forms of communication, because what is readily available on the internet for free is the type of communication that terrorist groups use themselves. Social media are probably the third biggest problem for us.

Next is the pace of technology. I touched on that with encryption. Technology is constantly evolving. We find it harder and harder to obtain information that we can use evidentially and engage in prosecutions. We work collaboratively with our partners to obtain as much of that information as possible, and use it collectively to help keep the UK safe.

The internet referral unit has been in existence for eight years. As I mentioned earlier, we have taken down over 300,000 videos. In the last week, we have removed 400 videos from the internet, so a large number of videos are still being broadcast on the internet. At our peak, 12 months ago, we were removing 2,500 videos a week. You can see the scale. It is often equated to the game whack-a-mole; we are constantly trying to identify where images are popping up on the internet and remove them.

We use a number of tools and processes, but, most importantly, we work very closely with those in the industry to try to educate and inform them about the risks of radicalisation, particularly in young people. The style of some of the videos being used over the last 12 months by terrorist groups is clearly targeting vulnerable young people who play games such as "Call of Duty", to make it look familiar to them. They are very slick and professional videos that are very appealing to young people. We are working with industry to make sure they can recognise such videos and remove them as quickly as possible.

With some of the bigger companies, we look to remove videos within 20 minutes. We estimate that, if we can remove the video within the first two hours, it will have a significant impact on the availability of that video globally. We think that after two hours the chances are that the video is out there; it has been downloaded and captured, and stored on people's devices, so we have less impact. That is not to say we will not continue to try to remove those videos and look for them elsewhere on the internet. We are very mindful of the pace at which we need to operate, and that we need to educate companies and industry so that they can work with us, realise the risks and have processes in place to remove material as quickly as possible and, importantly, prevent it being uploaded again.

Those are the key issues for us. I am happy to answer more detailed questions about any of those areas.

The Chairman: I thank all of our witnesses for those introductions,

which we are now going to pick up in a series of questions.

Q36 **Baroness McIntosh of Hudnall:** It is quite hard to take in everything you were saying, so this question might seem incredibly narrow, given the breadth of what you have all just offered us. All of you talked about working with the industry. Presumably, in relation to the videos you describe you work with YouTube, or whoever facilitates, by existing, the uploading of material.

To what extent are those platforms and companies protected by the e-commerce directive and do they have the safe harbour protections around them? In view of the fact that you work closely with them, you could obviously say that they are doing all right and they are not hiding behind that. At the same time, however, they have protections. Is it your view that the time has come for those protections to be changed or repealed?

Ms Susie Hargreaves: In relation to child sexual abuse, they do not have those protections under the e-commerce directive. Once notified, they are responsible for the content and must have it removed. One of the issues for us post Brexit is the loss of the e-commerce directive. It is quite straightforward in relation to our work; they do not have a place to hide. If we have assessed it as illegal, they will take it down, but they do it on a voluntary basis with us. As a self-regulatory body, we have no powers, but once they have been notified they are criminally liable for the content.

Baroness McIntosh of Hudnall: Can I emphasise the point you made in your written evidence, which is that, in the field where you work, there is no ambiguity about what is legal or illegal?

Ms Susie Hargreaves: Correct.

Baroness McIntosh of Hudnall: I imagine that in some of the other areas it is not quite so clear, but it works in your field.

Ms Susie Hargreaves: That is correct.

Mr Will Kerr: My answer is a bit more straightforward; it is yes. Now is the time to revisit the general protections given under the e-commerce directive. Susie is quite right; it is a bit more straightforward and binary when it comes to CSEA, but people are being trafficked throughout the United Kingdom at the moment for the purposes of sexual exploitation, and that is facilitated through adult service websites for which the hosting companies have no direct legal responsibility.

To make that real for you, very recently we had a case involving some men. One was convicted at the beginning of this year. It was a fantastic piece of work by West Midlands Police. A 14 year-old girl in Coventry had been advertised on an adult service website for £30 a month. The reason she ended up on that website is that she had been in care; she was a looked-after child with a significant range of domestic problems and had become drug dependent. She had worked up a £1,800 drugs debt. Her

drug dealer sold her debt to another drug dealer, who decided that as a 14 year-old girl she did not have the means to pay, and effectively took her into captivity in a house where she was guarded by a brother of the man. There was a very effective policing response, but in the four days it took to deal with the situation she had been forced to have sex with at least 20 men for between £120 and £150. That was hosted and facilitated by some of those sites. The sites have no vicarious responsibility for illegal activity that happens on them just because they happen to be a hosting platform. That needs to change.

Baroness Bertin: You mentioned in your introductory remarks that there were specifics that certain companies could do. Could you let us know very briefly what those specifics are?

Mr Will Kerr: I am very happy to. I am happy to go into detail on any of them. Sometimes, we cannot respond to the growing demands of the problem and we have to take a fundamentally different approach. That approach should be far more preventive in mindset. What could some of those companies do around CSEA?

They could do three simple things. One is that we could start to pre-screen or pre-filter some of the material before it reaches a hosting platform. The technological ability exists to do that. A significant proportion of indecent photographs have their own hash identities; effectively, the photographs have a digital signature. The known photographs that we have exist in what is called the Child Abuse Image Database in which there are over 9 million known and graded images. Let us plug one system into another and make it clear that, if you are responsible for hosting a platform, you must stop those images being uploaded in the first place and stop them being shared, and you have a proactive responsibility to take them down. That is a very simple thing that could be very effective.

Secondly, as the parent of a 13 year-old boy who spends more time on live-streaming and live-gaming apps than I would like, I would like to see some official means of kitemarking those systems by each of the companies. Not everyone agrees with me on that, but as a parent and a consumer I want to know that, when my son goes on to one of those sites, the company has signed up to three or four basic preventive steps and agreed to those design steps when it created new apps. Language algorithms have been developed that can identify grooming conversations with children. There is a developing AI space for some companies. We constantly look to prevent indecent images being uploaded to platforms servers in the first place.

If there was some form of official kitemarking, consumers and investors could make informed choices about the companies they want to invest in. I appreciate that it is a wide marketplace. It includes everything from a set-up by a 17 year-old in his or her front bedroom to multinational conglomerates. I appreciate that I am speaking generally.

Thirdly, perhaps slightly controversially, why would it not be possible for larger companies in particular to invest a certain percentage of their research and development budgets in preventing this happening on their platforms in the first place? If we can spend a certain percentage of R&D budgets on developing the AI that we know facilitates the encryption, destruction and anonymisation software that facilitates offending, why can we not spend an equal percentage of R&D budgets to stop offenders in the first place?

Baroness Kidron: I declare an interest. I am a member of the technical working group of the WeProtect Global Alliance in which Susie is also involved. My question is for you, Susie. Picking up what Baroness McIntosh said, is not the problem about the safe harbour? If you tell them that they have a duty to take it down, but they have no corresponding duty if they are not told and they can host whatever, is that not the crux of the problem?

Ms Susie Hargreaves: That is true, because we only know what we know, if you know what I mean. Once we know, we notify and action is taken, but one of the reasons we have a blocking list is that action is taken at a very different rate across the world. Action is taken very quickly in the UK, but it is not the same across the world. You are absolutely right; we would not know. Having said that, we get referrals from industry.

Could I say something about hashing? We work very closely with the Home Office, and we assess over half a million images for the Child Abuse Image Database. We have our own hash list and the Child Abuse Image Database hash list, which we supply to industry. Unfortunately, we are limited by the terms of a letter from the Home Office to share those hashes only with a number of US companies, but those companies upload all images. If you put an image on Facebook today, it will go through our hash list. Currently, there are about 310,000 unique hashes on our hash list.

Baroness Kidron: Can you explain why it is limited, just so that we understand it?

Ms Susie Hargreaves: The reason it is limited relates to when the agreement was originally set up. There is mandatory reporting in US companies and it is linked to that. If they find things, they go to NCMEC, which Will mentioned, and the reports come back to UK law enforcement. From our perspective, we want to be able to deploy the hash list across all industries so that they can use it to stop known images being uploaded.

Baroness Bertin: The implication of that is that the referrals will rocket up and go too high. Is that why they do not want to do it? Sorry, I do not understand.

Ms Susie Hargreaves: We do not have mandatory reporting in this country, so it closes the victim loop, with reports going from US

companies to US law enforcement, in relation to perpetrators and victims back in the UK, if it applies.

Baroness Kidron: There is something around "Don't look, don't see" and then mandatory reporting. I recognise your plea that, if it ain't broke, don't fix it, and the very good work you do, but there are some details around the edges that might tighten up some of the loops, or open up some of them, depending on how they fall.

Ms Susie Hargreaves: Clearly, we are covering only a teeny bit of the whole problem. The big US companies in particular have a whole range of technical services to prevent, block and disrupt child sexual abuse. Their search engines take our keywords. We have had engineers in residence from Google and Microsoft. Next week, we are attending a Facebook hackathon in San Francisco. They are very responsive to the area of work we are in. Grooming is a huge issue and the threat changes on a daily basis, but at the moment that is outside the remit of the IWF.

The Chairman: Do any of the other witnesses have anything to say before we move on?

Mr Will Kerr: The threat is changing almost on a monthly basis at the moment. We should not, particularly on the law enforcement side, be naive or complacent about the changing nature of the threat. We are struggling in terms of the capabilities we need to keep up with the criminals who are trying to exploit our children. It is now perfectly normative for a child to go into their bedroom after school and use a whole range of live-streaming applications and just live-stream their daily lives. The opportunities that that presents for offenders are fundamentally different from what existed even two years ago. We are now, on the CEOP side of the house, having to develop education packages for four to seven year-olds. We know that nearly a quarter of three and four year-olds now have access to the internet. The problem is getting younger, wider and more serious in nature and risk every single week.

Viscount Colville of Culross: Mr Kerr, you said you would like the platforms and internet companies to do more to develop preventive ways of stopping this from getting on to the net before it happens. Facebook and Google, and everybody, say they already have thousands of human moderators looking at content, and they are developing AI, yet it still does not seem to be sorting the problem. All we can do is look at this country, but do you think we should consider making it compulsory, if platforms want to operate in our country, that they contribute a certain amount of money towards preventive research?

Mr Will Kerr: A voluntary coalition is always better than a mandatory one, but the scale of the problem and the range of apps being developed by a range of different companies is such that to get any sort of consistency of response, that must be seriously considered. It is now a problem. We need to be very careful not to use hyperbole in this area, but we are deeply worried about the scale of the threat. The whole law

enforcement system is struggling to cope with the scale and nature of it. If we do not do something fundamentally different now, we will end up with the threat running ahead of us in the next few years. The short answer to your question is yes, we seriously need to consider it.

Baroness McIntosh of Hudnall: The overriding question is where and how the development of these technologies is happening such that you can get left behind. It is a naive question, but, as best you can, what is your answer? Where is the fundamental work going on that allows the technology to develop at the pace it is, and who is controlling that research? Is it happening in small pockets all over the place, or is it going on inside big companies and then being exported?

Detective Superintendent Phil Tomlinson: There is innovation all over the world in respect of app development, communication development and encryption. The most success we have had is through very careful and close engagement with companies. Some of the companies mentioned this afternoon are multibillion-pound operations with endless resources and budgets, but some apps are developed by one or two people in their bedrooms and sold to those companies, or used on phones.

It is important to make that point, because some companies do not have the resources to invest in some of the technology we are talking about, but we can work with them to educate them and help them have preventive processes. There is a responsibility on some of the large multibillion-pound companies that operate out there, but there is also a piece about collaboration and education with some of the smaller companies, getting them to work and engage with us in the UK and elsewhere in the world to ensure that they are not just protecting their customers' security and privacy, but that they are aware of the risks posed by some of the messages and communications going out from some of their customers. Close collaboration, education and training has been very successful for us in counterterrorism policing.

Chief Constable Stephen Kavanagh: The point that Will raised is really important. What we tend to do, certainly with terrorism, is look at legislation after the event, after some awful tragedy. Now we have an opportunity in the cold light of day, knowing the emerging challenge we face. Legislation or changes in procedures, processes, relationships and kitemarking made in haste after something awful are always less sustainable and less thought through than the opportunity we have today.

The Chairman: I note that your fellow witnesses broadly concur. We need to move to the next question.

Q37 **Baroness Benjamin:** I declare an interest as a champion of the Internet Watch Foundation. I would like to address my questions to Susie and Will. We know that every nine minutes a child is sexually abused online in material coming from somewhere in the world, including developing countries. Your driving mission, as you have both said, is to protect

children by taking down those sites. What process does the Internet Watch Foundation employ to safeguard human rights? For example, to what extent are individuals able to appeal your decisions to place URLs on a blacklist, and what scrutiny does CEOP exercise when giving you permission to issue takedown notices?

Ms Susie Hargreaves: When we find content, we locate where it is hosted. If it is hosted in the UK, which very little content is, we immediately notify CEOP, our referrals desk, and ask for permission to issue a notice of takedown. The best way to remove child sexual abuse is to do it at source. CEOP always has to give permission for us to issue a notice of takedown to ensure that we do not disrupt an ongoing investigation. The notice to take down is issued to the company in the UK.

If it is outside the UK, which the majority of content is, it is placed on the IWF URL blocking list, which is a web blocking list that blocks at webpage level. It is supplied at network level and deployed across the world. Today, there are 7,900 webpages on the blocking list, and we added 600 yesterday.

If you try to access one of the webpages on our blocking list and you live in the UK, you will be served a splash page that gives you a number of pieces of information. It tells you why you have been blocked; that the page has been assessed as illegal content; what to do if you are worried about your behaviour; the potential ramifications of your behaviour; and what to do if you feel you have been blocked in error.

We have a formal appeals policy. Four years ago, Lord Macdonald conducted a human rights review of the IWF and made a number of conclusions, including that we were human rights compliant and subject to judicial review. We had a complaints and appeals process in place, and he recommended the engagement of an independent inspector. We now have Sir Mark Hedley, a former High Court judge, as our independent inspector to oversee any appeals. That is made clear on our website, and it is made clear if anybody contacts us. The appeal process applies across the world.

Mr Will Kerr: The IWF is an independent organisation; it is not an extension of law enforcement, so the NCA does not direct or regulate IWF activity. We provide a method of de-confliction with law enforcement. At times, there may be operational reasons why we do not want to issue a takedown notice and we work very closely with the IWF on de-confliction.

We have a very strong and positive relationship with IWF. To give you a sense of the scale of the number of referrals we get, last year, in the financial year 2017-18, we had 1,160 reports from the IWF, of which 41 related to sites within the United Kingdom. As Susie said, most of them relate to international sites outwith the United Kingdom.

Baroness Benjamin: How many requests for appeals do you get?

Ms Susie Hargreaves: Hardly any. If we get requests, often it is because the list has been deployed inaccurately by the industry member. Someone may have been blocked and it has nothing to do with us. We have had no appeals go forward in the last couple of years.

The Chairman: There has been no fundamental appeal against your decision; it is usually because of an error.

Ms Susie Hargreaves: Correct.

Baroness Benjamin: I was interested to hear you say in your opening remarks that, if it ain't broke, don't fix it. What action would impede or harm the work you are doing at present? Why did you say that?

Ms Susie Hargreaves: Because child sexual abuse is very clear in law, and we are able to assess and our judgment is trusted; we are able to remove content at a speed that is unrivalled across the world. If we had to get a court order and a judge to decide it, the content would stay up for weeks. Our view is that it works incredibly quickly. We are a trusted organisation and we can move very quickly and get content removed so that a child is not revictimised, but we recognise that that is not the same for all internet harms. Different content needs different approaches. We benefit from absolute clarity of purpose, which is backed up by UK law.

Lord Gordon of Strathblane: In your written evidence, you mention that you get no money from the UK Government, but you get between 10% and 15% from the EU. Do you think you should get money from the UK Government, or do you think it would in any way compromise your independence if you did?

Ms Susie Hargreaves: That is a very good question. We get money from the EU as part of the UK Safer Internet Centre. We are part of that, with our partners Childnet International and the South West Grid for Learning, which provide awareness-raising and a helpline.

We have traditionally always stood away from receiving money from the UK Government because of our self-regulatory status. However, we are in ongoing discussion with DCMS about what happens to that funding with Brexit. Given the percentage, we have a legal view that it would not affect our self-regulatory status, but we do not have an absolute position on it yet.

Lord Gordon of Strathblane: Another point you make in your evidence is that stuff that is harmful and should be removed from the internet should be clearly defined in law and not subject to discretionary subjective interpretation. Surely, that has been the very basis of your success. People trust your judgment and abide by it. If you start defining it in law, somebody will wriggle out under whatever regulations you have.

Ms Susie Hargreaves: With respect, we would not say that our judgment is subjective; it is objective. When we look at an image, we ask whether it meets the category A, category B or category C criteria. Category C is much more open. If we are in doubt, we take a legal

opinion on category C, whereas with hate speech, or other areas of internet harm, there is a level of subjectivity that we feel does not apply to child sexual abuse. If a child is engaged in a particular sexual act, it will automatically reach the thresholds of A, B or C.

Lord Gordon of Strathblane: To put it beyond doubt, if you said what I think you said in answer to Baroness Benjamin, when you say, "If it ain't broke, don't fix it", that applies to what you are doing; you are not suggesting it as a solution to the other problems that have been mentioned.

Ms Susie Hargreaves: Certainly not. They are all very different and need different solutions. The internet industry would benefit from clarity about the different areas of internet harms. One of the reasons companies work with us is that there is absolute clarity, but I am totally not saying that the IWF solution is the right one for every type of harm.

Viscount Colville of Culross: I would like to broaden my question to abuse not just of children but of adults. We received a very interesting submission from the Australian Office of the eSafety Commissioner, which has set up a two-tier system. In the first tier, it co-operates with the platforms and they are signed up, so they have a mutual relationship, but the second tier is for those who decide not to co-operate, and they are subjected to legally binding notices and penalties. Chief Constable Kavanagh, do you think that scheme might work in this country?

Chief Constable Stephen Kavanagh: I am not aware of the system, but it appeals to me. We have talked about the hate crime, bullying, harassment and gang-grooming that is taking place on the internet, and one of the challenges we face is that there is a spectrum of harms taking place. In any system we bring in, we have to recognise that the majority of the major providers will want to create an environment where their users are safe. Are they doing enough? I do not think they are. Will suggested that a small proportion of their profits is used for R&D and creating a safer ecosystem for their users. Is that sensible? Absolutely.

The challenge we face is that, every time we address one of the harms that is taking place on the web in its broadest sense, it mutates into something different. We need the ability to work as constructively as we can with the main providers. We have heard some really good examples of how they want to work with counterterrorism; they work very effectively on intellectual property issues and child sexual exploitation. Those principles now need to be underpinned to deal with hate crime, harassment, gang behaviour and other things. Any system should recognise the opportunity to do some voluntary work, but when it is not being conducted in the way we would wish, there has to be some bite in the system, because nice conversations have not yet got us where we want to be. There needs to be a bit of grit.

Q38 **Lord Goodlad:** Chief Constable Kavanagh, could you tell us how you distinguish hate speech and other offences, where a key element is abusive, hurtful or unwanted communications, from speech that is merely

offensive, if there can be "mere" offence? Secondly, what factors do you take into account when deciding whether to notify companies that they are hosting illegal content, or whether to refer a case to the Crown Prosecution Service?

Chief Constable Stephen Kavanagh: Thankfully, following the awful events, and the poor response to them, over Stephen Lawrence 25 years ago, the advice to police is that everything to do with hate crime reporting is subjective. It is not for the police to test the victim as to whether or not a middle-aged white chap or a young white woman understands what it is like to be subject to those types of crime. Clear guidance has been published by the College of Policing to make sure that the moment somebody reports that type of crime, the police understand its impact. There is a cumulative effect of hate crime. The trouble is that previously, policing tried to look at a comment, or a series of comments, about an individual in isolation. These things impact on whole communities, whether it is a Muslim community or a black community, or whether it is based on religion or anything else.

What we have tried to do in policing is not just to impose greater rigour in allowing victims to explain why something is a hate crime. Through the True Vision website and other reporting forums, including local community hate crime reporting, we have enabled people to come forward and not be judged by the police in the first instance. We try to understand what has taken place. Why did they understand they were being targeted? What has previously taken place? Who is a suspect? What has taken place on a social media platform, perhaps around tattoos, language and regalia, that might be in the background for us to understand what reinforces it?

The police are clear that we are not the arbiters of good taste. If we were, Frankie Boyle would be out of business straightaway. We try to understand why hate crimes take place. The challenge facing internet providers, service providers and the police is that they are being ignored. People do not have confidence in the system; they are not reporting sufficiently, so there is a huge gap in our knowledge about the vitriol and nastiness that takes place on social media platforms. A lot of people disengage from them. They might block people. A range of activities takes place.

For broader abusive language and distasteful conduct, the CPS has rightly set the threshold for police or criminal prosecution very high. The inappropriate and stupid comment, or inappropriate joke, that somebody used to make in a café or pub and is now published on social media is a world away from hate crime and somebody being targeted because of their difference. But the CPS is clear that it will support the police when the victim has identified that something is a hate crime and that is the motivation behind it.

We usually go through the NCA and other bodies to make sure that the process is put in place. On the whole, we do not get the same response as to child sexual exploitation or counterterrorism, but in due course, if

we can identify it as a hate crime, the providers usually give us the evidence to present to a court. The CPS is supportive, but it does not want to get engaged, and it does not want us to get engaged, in inappropriate humour and distasteful issues. Our responsibility is to eliminate discrimination and identify harassment, and make sure that victimisation is dealt with at source as quickly as possible.

The level of training is a challenge. I have changed recruit training for my new officers so that they become more digitally confident in what they are expected to do. If we have a stolen car, the idea is that a crime scene examiner takes fingerprints or DNA, but in that car there are telematics systems and Bluetooth technology that will give us a far clearer indication of where the car has been and whose phone has been on while they were trying to steal it or commit a crime in it.

I do not think we should sell the hate crime piece too strongly. I am deeply concerned that we keep alive the memory and experience of what happened to the Lawrence family and black communities, because it becomes a cyclical issue. Police fall short; communities become disfranchised and angry with policing. We need to keep an eye on hate crime on the internet.

Q39 **The Chairman:** You might argue that hate speech which does not meet the threshold for hate crime is not a policing matter and is a matter of taste, so this may be an industry question. Does the industry have a consistent view when it applies its community rules, for example, about what constitutes hate speech and speech that is inappropriate for its platforms? Are companies looking for leadership in that area from politicians or policymakers? Susie, can you help us with that?

Ms Susie Hargreaves: I do not think they are consistent, because everyone has different terms and conditions. This is probably an area where some clarity will be very helpful to industry, but for lots of types of content companies have their own terms and conditions.

Mr Will Kerr: It is a very difficult space to legislate for. Separating intent in the use of language and behaviour that, as Steve rightly said, would have happened in the street, in shops and in face-to-face encounters from intent in what is now happening online—those are fundamentally different. We need to think about it very carefully.

An average 16 year-old today spends between 60% and 70% of their time communicating with another human in a virtual space; they do not do it in the way you or I may have experienced growing up—presuming you are in my age band, which is very presumptuous. We need a fundamentally different set of laws that reflect the experience of children growing up today who communicate, think, act and speak fundamentally differently because it does not involve eye-to-eye or face-to-face contact. That is a different human dynamic, and our legislative base needs to evolve to reflect it.

Lord Gordon of Strathblane: We have heard some evidence that what

the Germans have done, for example, has gone slightly too far; the pendulum has swung too far in the other direction, which will inevitably produce a recoil effect. Do you agree?

Mr Will Kerr: I do not know much about the German experience, so I cannot make an informed comment on it. All I know is that, as Steve hinted, the CPS has set a sensible and necessarily high threshold for hate speech. Balancing that with the need for free speech in a liberal democracy is difficult. Of course, that is not for us as police officers; we enforce the laws that legislators set, but it is a very difficult balance, which is evolving at a pace we struggle to keep up with.

Chief Constable Stephen Kavanagh: There is a massive opportunity for companies to use AI more effectively in some of these areas—machine learning concepts of abuse. At the same time, as we were discussing earlier, we have words that we may have experienced as inappropriate and would flag up as inappropriate behaviour, but on the rap scene there are hugely abusive slang terms on social media that would mean absolutely nothing to most of us in this Room, so we need the ability to adapt.

There will not be a silver bullet. Whether or not it is the AI piece identifying blatant language, we need to be able to update it and understand it, but then it will be turned into a song format or another format. Differences between gangs used to be an argument in and around a park; now they are embedded in social media, leaving lasting antagonism between groups, sometimes in very subtle ways. That is driving violence not just on the internet but in some of our local communities.

Baroness Kidron: My question follows on from your last comment, Chief Constable. I was going to ask about the culture of the internet the other way round. We all support the high bar of criminality, but is there something in the design of services, in signing up to better terms and conditions, in moderation, in mediation and quicker response time? Is there something that companies could be doing to detoxify their own environments, so that perhaps there is not a huge push towards something that may or may not become criminal in the end? It is not putting blame on them but putting responsibility in that place. Do you feel that is the case?

Detective Superintendent Phil Tomlinson: There are things that can be done. There is a huge range of different terms and conditions and different legislation in different countries. The internet is global and there are many companies operating in different parts of the world. Some of the large US companies are very particular about protecting their freedom of expression. A video that we say is offensive and may be hate speech in the UK may not be considered to be so in the US, so there could be reluctance to remove it.

However, to go back to the point about education and information for companies, they have technology that can block access to websites from

the UK. IP addresses in the UK can be blocked from accessing videos. Some stuff can be done by the companies. Even if there is no breach of their own terms and conditions, they can understand that there is legislation in the UK and technology in the UK to prevent access from the UK and protect our UK interests, even though it is accessible in the US.

Mr Will Kerr: There is no easy answer, because it is a very difficult issue. Being able culturally to translate into online communication and engagement the level of respect you would have for an individual when having a conversation with them in real time in the real world is a bit of a challenge. Phil is right. We can address the level and ease of anonymisation that sometimes makes it easier for people to hide behind virtual proxy networks, or whatever they happen to be. There is an issue about consequence, which is something that will concern you significantly. Making sure that it is harder to hide behind VPNs or a range of other technology tools to spout hate language and, on the other hand, making sure that there is a wider range of deterrent consequences are tangible things that perhaps the system could do.

Q40 **Lord Allen of Kensington:** Detective Superintendent, how do you distinguish terrorist content on the one hand and legitimate speech on the other? I am particularly interested in where the content endorses conservative religious views? What factors do you take into consideration when you are looking at whether to notify a company or refer a case to the CPS?

Detective Superintendent Phil Tomlinson: We have a number of methods to identify what might be terrorist content or extremist content online: referrals to the Action Counters Terrorism website; public referrals using the anti-terrorist hotline, Crimestoppers or a local police station; or referrals through other agencies or charities. There is a huge range of areas where people can make referrals to us to highlight their concerns about content they think may be terrorist or terrorist-related.

We also have our own processes in place where we can look across the internet and search for what we think may or may not be terrorist content. Once we have obtained information and looked at it, we compare it with the database we already have of what we know is terrorist material, either because it has been used to support prosecutions or because it has already been looked at by the Crown Prosecution Service.

We look at the terms and conditions of the company. You may click the box to say, "Yes, I've read the terms and conditions", but we are some of the few people who actually read them and go back to the company and say, "We've looked at this material. We assess it to be a breach of your terms and conditions and we ask for its removal". At the same time, if we think it has reached the threshold of criminality, we refer it to the counterterrorism division of the CPS. It is not a case of doing one or the other; we look to do both.

The CPS makes a decision on whether or not it believes it is terrorist content. We will already have captured it evidentially and obtained as much information as we can from it, and looked to enrich it with additional communications data we obtain from the company to try to identify any suspects, if they exist. It is not a case of doing one or the other; it is a case of looking collectively across the data. Do we already understand and know about the data? Is there more we can do to enrich the data? Then we work with the companies to highlight the risk to them because there is a breach of their terms and conditions or of UK legislation.

Historically, companies were keener to remove content if it breached their terms and conditions, because of the impact on markets and advertisers, than if it potentially breached UK legislation, particularly if they were based overseas and not governed by that legislation. That has improved, particularly over the last 18 months, and we now see fast takedowns by companies.

Lord Allen of Kensington: Do you see it as binary? Is it either terrorist content or not, or is the model similar to the A, B and C content model in a different environment? There must be a grey area, which is always the difficulty. Do you have any insight on that?

Detective Superintendent Phil Tomlinson: A good example would be where a major online news outlet puts out an Islamic State video. The same video could appear on a terrorist website and we would say that it had terrorist content and would look to remove it. Often, it is the context—the narrative that goes with the speech and the way it has been advertised or presented on the internet—that makes the difference between distributed and publicised terrorist material and journalistic material.

It is a very fine line, and more could be done to work with online news agencies in particular to inform and educate them on the risks of publishing such videos, which potentially reach a far wider audience than the people who find them on file-sharing sites, which might be quite obscure on the internet or could even be on the dark web. A lot can be done to work with some of the big agencies to educate them to understand the increasing risks of putting out that material.

Baroness Bertin: I should have made a declaration earlier. I work for BT.

I want to pick up a point Susie Hargreaves made about education, particularly on live-streaming. How good do you think sex education, which will be compulsory from September, is on that issue? That will be so important. Children need to understand the potential of what they are doing.

Ms Susie Hargreaves: Absolutely. It is important to raise awareness of the issue. We hear the phrase "building resilience online", but we are dealing with child sexual abuse from nought to 18. You can build the

resilience of a 16 year-old, but you cannot really build the resilience of a one year-old, so you have to take different approaches.

As Will mentioned earlier, we published a report today about the use of webcams in bedrooms. We have seen children as young as three in bedrooms. Clearly, they had been coerced to take part in some really bad acts. We need to do a lot of work on the educational side so that parents and families are aware of the implications.

Baroness Bertin: Do you think schools are really aware of how serious it all is?

Ms Susie Hargreaves: Increasingly so. We are a third of the CSEA of the UK Safer Internet Centre, and we also run the UK Safer Internet Day in February of each year. Increasingly, there are great campaigns by the NSPCC and others, and there is CEOP's Thinkuknow initiative. There is a mass of resources, but the fact that it is coming into the curriculum will definitely help. The internet safety strategy will raise awareness, but there is still much more to be done.

People do not realise that children are at risk even in their own homes. One of the videos I watched was of a child of about 10 in her bedroom; I heard a parent shouting, "Dinner's ready", and a category A act was taking place. We have talked about technology, but where you have a camera-enabled device and an internet connection there needs to be education. Children need the right level of supervised access to those.

Q41 **Baroness Bertin:** You touched on resource in many of your comments. Do you have enough resource, and how sustainable is the level you have at the moment for the increasing volume of work you are all having to deal with?

Mr Will Kerr: My sense is that the resources are not looking at the problem in the round and we need to take a different approach. We have a tendency to treat the problem simply as a law enforcement problem that requires a Pursue response. That is fundamentally not working in the CSEA space at the moment and we need to be able quickly to recalibrate far more effort and investment into the Protect, Prevent and Prepare space. Using live-streaming in compulsory sex education is a very good example of how we need to involve a range of other government departments outside the traditional law enforcement space.

Under the Thinkuknow education platform, CEOP is developing a package called live skills that deals directly with live-streaming risks. It aims to do a range of things: educate children, parents and carers about the tactics used by offenders; think critically about people met online; respond to pressure and manipulation online; and deal with low confidence and self-esteem issues that can make children vulnerable in the first place. Those are not unilaterally policing responsibilities, but at the moment the system is designed such that we struggle to separate the issues that make children particularly vulnerable—although it is not just children—to online exploitation and abuse, from the criminal exploitation that

fundamentally and clearly sits within the law enforcement space. We are cramming in too much responsibility, and the system is struggling to cope.

The Chairman: Chief Constable, you spoke earlier about effective co-ordination between police forces. We have just heard that there is probably insufficient co-ordination across wider society, government, schools and education. Where should that be taking place? First, is that forum obvious to you? Secondly, what about resources?

Chief Constable Stephen Kavanagh: I do not think there is sufficient co-ordination. There is a real opportunity for us to look at policing and law enforcement more broadly. We are trying to come together, whether on standards for data analytics, standards for information management or approaches to victims. At the National Police Chiefs' Council office, there are probably about 10 people trying to develop some strategic thinking. Either we place it with the Home Office and ask the Home Office to take some responsibility for these issues, or we say that the police chiefs, under the leadership of Sara Thornton, have a bridging role to play in showing strategic leadership in this area.

In the NHS model, the Caldicott principles for data management are interesting. Trying to set down something for the NHS on the strategic management of data nationally works very effectively. Where is law enforcement in establishing a similar model to ensure that we consistently apply those issues? This is a really important time for us. Either the Home Office needs to step up and take responsibility for some of the issues, or we need proper resourcing of the National Police Chiefs' Council, or some other set-up, to inform how we move forward in a more considered way.

We have witnessed the outcry over Cambridge Analytica and others. As policing moves into the digital age, it must maintain its consent; it must understand where it can go in the digital sphere with the support of the public. If it goes too far, we will lose the consent that is so important to the British policing model.

On resourcing, my force had 3,600 officers; it has gone down to 2,800 officers. In addition, we lost three-quarters of our police and community support officers. We have lost about 1,000 uniformed people on Essex streets. At the same time as we have been losing those staff, I have had to find officers to place in cyber teams and additional fraud teams, and to try to develop their skills in online investigations and work with the NCA. They come from community policing and local response teams.

At a time of reducing resource, we have had to pull resource out to start to manage some of those concerns. Policing is becoming increasingly thin and it is not dealing with community issues in the way it would wish and with the speed of response it would like; nor is it dealing with the digital sphere. Unfortunately, at the moment, if we are honest, it has all been stretched too thin, and we need to think about whether or not it is a sustainable model.

Baroness Bonham-Carter of Yarnbury: At the beginning, Detective Superintendent Tomlinson referred, in a very visual way, to searching for multiple pins in multiple haystacks. To pick up what you were just saying about the digital sphere, what technological tools can you use in law enforcement and, when you use those tools, what human oversight is required?

Detective Superintendent Phil Tomlinson: I mentioned some of the volumetrics at the start, with some of the larger terrorist investigations involving 35 terabytes of data. That is a big investigation, but typically we seize that amount per month. I talked about piles of paper. The entire British Library is 32 terabytes, so, in mainstream police investigations, we are often asking a police officer to read the entire British Library to look for evidence. We are also asking them to look in different parts of the world. Some of the books have been torn up and destroyed and we want them to put them back together again. That gives an idea of the scale of the problem the police face with regard to digital evidence and how they can produce it and understand it. That is just one investigation.

A typical police officer working in a borough will probably be dealing with 30 investigations. If we multiply the British Library by 30, we see some of the issues and challenges that the police are facing. There are no more resources to deal with it.

Baroness Bonham-Carter of Yarnbury: Presumably, you need language skills too. That is not necessarily something we are greatest at as a country.

Detective Superintendent Phil Tomlinson: Absolutely. In a lot of our investigations we are reading Arabic, so we have translators. We invest in translation tools that can assist us to triage data. The big problem for us, which I mentioned at the start, is around encryption. Sometimes, people oversimplify the issue and think you can download the content of a phone and then it is just a case of reading it as though you were reading the content of any other phone. It is not as straightforward as that. If you printed the content of your own phone on a piece of paper, you would not be able to make sense of it. The conversations you were having in a chat group would make no sense, because you would be seeing them on multiple spreadsheets. It is very hard to contextualise information and make sense of it.

Another issue is that a lot of data is not stored on devices but on a cloud elsewhere, so people no longer throw away their data. Five or 10 years ago, if your phone had 100 text messages on it, you would have to delete them. People do not delete information any more. It never disappears. They just upload it to the cloud and rent more space for 49p a year. They are collecting more and more information, which could be across 10 different devices because they upload it to the next phone, and then the next one and then the cloud. That presents lots of challenges for us.

There are tools we can use. Steve mentioned artificial intelligence. We can use that to assist in understanding what the evidence is and look for

it on our behalf, but it is simply a system of triage. We still have to look at it and make an assessment, in the same way as internet referrals. We have to look at the information and make a human decision on it. It is not a case of AI finding and presenting evidence for us. That is a real challenge. Counterterrorism policing is luckier than many, but wider mainstream policing is facing challenges around that. In answer to your question, we need resources and technology.

Baroness Bonham-Carter of Yarnbury: Maybe more resource would help in developing algorithmic processes; it could help with person power.

Detective Superintendent Phil Tomlinson: It would help to some extent, but sometimes you cannot throw more resource at the problem. An interesting comment made to me last year was that more data would be seized in police investigations in the next two years than there are people in the UK to view it, so it will not be possible to view all the data. That is one of the issues we have to face. Chucking more resources at the problem is not a long-term solution. It might work in the short term, but in the medium to long term, we need smarter technologies.

Baroness Bonham-Carter of Yarnbury: I meant resources directed at developing smarter technology.

Detective Superintendent Phil Tomlinson: Yes. There are companies working on developing that technology, but they realise the value of it and, therefore, it comes at a price greater than the police can afford to pay.

The Chairman: There were some incredible superlatives in your presentation.

Baroness Kidron: We talked specifically about the resilience of kids, but that could go across the board. We have just talked about the technology available to people who are trying to tackle the problems. The Committee has been very interested in a sort of design-to-be-well, design-to-be-safe and design-for-society idea. What sparked my interest was the live-streaming example. What if live-streaming automatically came with switch-on and safety? Presumably, if people were determined to do harm, they would do it, but a lot of the low-level availability that live-streaming allows would be knocked out, or at least, there would be education pieces. Do you consider design-to-be-safe in any of your areas as a responsibility of industry, or at least as a new place where we could all look for some negotiated settlement?

Mr Will Kerr: I think Baroness Bertin touched on this earlier. The whole system needs to be fundamentally recalibrated. At the moment, the model is too focused on a reactive response to a growing demand that we cannot cope with. It is not focused enough on growing the capabilities to deal with the higher-end risk. We know the break point in that. A significant determinant of the break point in that model has to be the responsibility of industry to deal with preventable offending in the UK, and allow us to accelerate our capabilities to deal with some of the

higher-risk offenders here. That is the fundamental problem we face at the moment.

The academic Matthew Falder was convicted in February this year. To give you a sense of the scale of that investigation, the NCA led an international task force. It took us four years to catch him. It involved a wide range of international partners and a range of covert capabilities that we had to develop ourselves. It still took us four years to catch him. That is one offender on one particularly horrific site, but with at least 300 victims worldwide. If we do not deal with the preventable offending side of that spectrum, we are not going to be able to deal with the likes of Matthew Falder, who pose a far greater risk of significant harm to a wide range of vulnerable victims.

Chief Constable Stephen Kavanagh: A whole series of guardian communities are springing up in and around the south-east at the moment. Every single one of them is underpinned by designing out crime with processes, expectations and regulation. We should not underestimate the fact that the communities that our children, our parents and we live in when we are not in this Room are as valid today as the ones we go home to when we are sitting in our houses. We have to make sure that those communities are based on the same principles that apply in the physical lives that we lead.

Baroness McIntosh of Hudnall: I want to ask Mr Toon about areas of criminality from which we need to be kept safe that are not of the sort that make us all feel deeply sick. Child sexual exploitation is deeply emotive and catches us all whenever it is discussed. What about issues to do with cybersecurity in other areas, such as our financial protection and the way the whole economy is vulnerable to significant disruption? We know that inside this institution we are regularly under attack. We are usually okay, but sometimes we will not be.

Are we sufficiently equipped with resources, whether legislative, technological or whatever, to look at other areas of criminality, or harm that may not necessarily be criminal, against which as a society we need to be able to defend ourselves, possibly pre-emptively?

Mr Donald Toon: You raise a range of issues, but many of the answers are very similar to the position on child sexual exploitation. A fundamental issue touched on earlier was around education. That is absolutely critical in the prevention of live-streaming vulnerability, but there is something about the wider ability to be safe and secure online, for people to have a fundamental understanding of the risks they and their families are running.

We see a specific problem from a cyber perspective. We have developed tools, communication and training so that parents can identify risks, such as the classic young teenager who moves from a very strong focus on gaming and crosses a boundary where it is no longer online gaming. They are no longer focused on, "How do I throw people out of the gaming structure that I am doing online?" They start to challenge websites and

the operation of legitimate industry. We have seen a number of very significant incidents where young people have found their way into criminality because there was no educational process to identify the risk of them doing so. We have seen people slip into that form of problem.

We also have a fundamental problem around online financial safety. It is very clear to us that online-enabled fraud is currently the most common crime in the country. It is a crime we are most likely to be impacted by. It is also an area where the law enforcement response is probably most limited in its ability to be effective and impactful. Most of it is carried out from overseas; it manifests itself X million times inside the UK. Each time it is a few hundred pounds, but it is not X million separate offenders. We are talking about organised criminality on a worldwide scale, carrying out thousands upon thousands of offences, each one worth a few hundred pounds. That is a huge issue and the amount grows.

It is a huge issue for all the individuals involved; it is a huge problem from the law enforcement perspective. It is the same issue about education, understanding, ability to appreciate risk and ability to use some of the tools that are relevant in respect of child sexual exploitation, counterterrorism and hate speech. It is the ability to identify where fake websites are being used, such as those where people are defrauded of their pension pot and conned into investment structures. In all of those, there is the opportunity to use a similar set of tools around breaching terms and conditions of service for hosting websites and taking down websites.

There is a continuous process, but it has to be balanced between law enforcement, and the regulatory and control structure around the provision of hosting services, and the knowledge, awareness and understanding of risk of the public at large. The same tools and the same issues very much apply. The criminality is not of the horrific kind we have been talking about in the case of sexual exploitation, but its scale is significantly greater. That leaves aside direct cyberattack and cyber-risk. There are some real issues which it is important to get to grips with. It is important not to be too siloed. When we talk about trying to protect young people and increase their understanding, it needs to be about how we can live a safe life online.

Baroness Benjamin: In your opening remarks, you mentioned money and people being prepared to pay to see child sexual abuse online. How do they pay for it? I presume it is through a credit card. Should credit card companies have some sort of responsibility?

Mr Will Kerr: We are starting to see a slight shift in the risk factors involved with CSEA, whereby live-streaming gangs that exist to make money, a significant proportion of which are in the Far East, are engaged in CSEA. As I said in my opening comments, they are not sexually motivated, although some of them might be; in the main, they are in it to make a profit.

There are significant investigative opportunities and, therefore, significant disruptive opportunities in the fact that these are not just normal banking transactions. There is a whole range of both direct and anonymised money transfer systems online at the moment. I do not want to talk about them in too much detail, because the more they are used, the more we can, hopefully, disrupt and catch them. That is what we would like to do, but there are a number of different ways in which they transfer money at the moment.

Baroness Benjamin: What can be done about it? Surely, the organisations that are involved as far as the money aspect is concerned have some sort of responsibility, because they are dealing online, too.

Mr Will Kerr: Absolutely. Because this is very much an emerging and evolving element of the CSEA threat, what we have to do in the law enforcement space is develop a suite of standards that will help prevent it in a systemised way across the whole of the banking transfer industry. That is exactly what we are doing at the moment. We are trying to look at diagnostics across the system that would indicate small transactions.

For illustrative purposes, perhaps a 50 year-old man in Bradford is making multiple payments to the Far East on a regular basis. If nothing else, that might be suspicious. If it is, we need to understand how we aggregate all the diagnostics to do disruption through the money-transfer industry and not unnecessarily criminalise that 50 year-old man, who may have a business interest in the Far East. It is a careful balance, but there is a developing range of tools that we are engaged in at the minute. I just do not want to talk about it.

Q42 **Baroness Kidron:** One thing that keeps coming up is that, if somehow we work to smart standards, good ethics, regulated behaviour and terms and conditions that everyone keeps to, everything that is difficult will move to the dark web. We are interested to know your collective or individual views on that, so maybe you could all answer slightly different pieces of this question.

A subset is the role of encryption, which many people feel protects them from the intrusion of commercial companies in their personal lives, but perhaps presents a problem for people who are looking for things that should not be going on. Do you have any views, either institutional or personal, on the balance between law enforcement, encryption, transparency and the rights of business leaders? I know it is a very broad question.

Mr Will Kerr: There is no longer a binary distinction between the dark web and the open web, and Donald will no doubt be able to explain that far more effectively. The only point I would make, and I am sure Steve would make exactly the same point, is that the levels of encryption that are now standardised and de rigueur, and were not the case even three or four years ago, have a massive impact. The intensity of the law enforcement investigations and the resource investment we have to put in to catch the same offenders fundamentally changes the law

enforcement investigative model. If we are to concentrate on risk, which is what we should be doing, we need a better way of preventing volume demand, to allow us to do that. On the distinction between dark web and open web, I defer to my colleagues.

Mr Donald Toon: The fact that we are able to reach a situation where the surface internet is a safe environment and that that potentially corrals problematic behaviour into subsidiary areas is valuable in and of itself. It starts to create greater consciousness among people that if they are moving into an area that looks like the dark web—the Onion router, or whatever kind of space they want to get into—they are making a conscious choice to move into an identifiably high-risk area. They are drawing a distinction between that and a safe operating environment.

There are about 30,000 sites on the dark web at the moment, of which probably 50% are engaged in, or facilitating, some form of illegal activity. Linked to that is the use of particular forms of cryptocurrency to facilitate payments and movements around the dark web. There is a whole range of issues about the ability to investigate, operate effectively and follow payments. It is a very long and complicated subject to get into. It is really important to make sure that we have a co-ordinated and effective law enforcement effort to tackle the dark web, and that we do so not just on a UK basis but internationally. Working with international partners is hugely important. The vast majority of developed countries face exactly the same problems and risks, and we partner effectively on the dark web.

Linked to that is the wider debate on control and regulation of virtual currencies, which are used very heavily in support of dark web transactions. They are certainly used very heavily in the purchase of a whole range of services—everything from child sexual exploitation to firearms supply, money laundering and major fraud. Currently, we have a situation where an entire financial and payment structure is not subject to the same regulations and controls as normal currency.

We have to be quite careful. There is an advantage to some extent, in that people know they are taking a risk if they get into virtual currencies, but at the moment it is important to make sure that there is more effective control in the virtual currency space and that we have a harnessed and mutually supportive international effort to investigate and share information and intelligence on the dark web. The more we can make the surface internet a safe place to operate, the more effective and targeted we can be, and the more we can encourage people to understand that the dark web space is fundamentally a risky area in which to operate. We could have a long debate, but that is probably the easiest and shortest way to cover it.

The Chairman: Are there any benign reasons why anyone would want to be on the dark web and, if so, could you briefly explain what they are?

Mr Will Kerr: Maybe a journalist working in a hostile country.

The Chairman: The assumption that everything on the dark web is in

some way a problem does not work.

Mr Donald Toon: But it carries a risk. You still have a situation in which people are on the dark web because they know they are facing a series of specific risks. They are not in the dark web simply because they drifted into it.

Chief Constable Stephen Kavanagh: Donald did a really good job. We want the surface web to be safe for our children and for us to be able to do our banking and engage in social media, and we need to focus on greater understanding. I have struggled with the idea why in this country, if you are not an academic researcher or a journalist, there are reasons for having an Onion router to get into the dark web. Why would my son, or anybody else, want one of those pieces of kit in this country at this time? It is an important question for us to ask. We do not want to limit free speech and we do not want to limit people unnecessarily, but we need to understand why they want to go on to the dark web. There might be a justification for it, but we must focus on the open web at the moment because, if we try to take on too much too quickly, we will fail. We need to focus our efforts on mainstream society.

Ms Susie Hargreaves: I agree with everything that has been said. Although our remit is limited to the open web, we work within the dark web a lot because we are able to access and hash the images, and many of the images in the dark web are linked to image-hosting boards that are available on the open web.

The opposite of the dark web is that there is a real danger that we forget old technology. Last year, we saw the biggest use of newsgroups since we started. Newsgroups are one of the oldest chat-room technologies. There is so much content still out there on the open web, and we should not lose sight of it.

Baroness Kidron: Because it is a broadly held view, or at least a broadly held answer against regulation or community standards, that everything will be pushed there, do you think it is a disingenuous view? I agree that there are many decent reasons for being on the dark web, but at least you know you are in unfettered space. Do you think it is a disingenuous argument, which is quite mainstream, that if you clean it up upstairs it will all go downstairs?

Mr Will Kerr: Yes, in part. Matthew Falder is a perfect example. He, along with people who were so inclined, was able to use so-called hurtcore sites on the dark web to amplify the threat to children on the open surface internet. We need to understand the relationship between the two, as Donald explained so well earlier. Matthew Falder operated on hurtcore sites where people were able to share vile images. It was not just sexual abuse of children and adults; it was a level of degradation and humiliation they wanted to get them to engage in. Donald made the point that they had to exit the surface web to go on to the dark web to share that material with like-minded people, so the dark web has the ability to

amplify the open surface threat. We need to understand that relationship a lot better.

Viscount Colville of Culross: Mr Kerr, we had an interesting submission from Leicester University. Its concern was vulnerable workers on the internet for whom working on platforms can be quite beneficial, such as sex workers. Its concern was that, if you over-regulate adult service sites, you might destroy the beneficial aspects for sex workers of being online and drive them underground. Do you have anything to say about that?

Mr Will Kerr: It is a challenge. There are a number of adult service websites available in the United Kingdom at the moment. In the United States, they have taken a slightly different approach with their FOSTA legislation, and closed down one site recently. They realised that a number of sites were facilitating the trafficking of people who may have presented as willing sex workers but clearly were not; they were vulnerable and were clearly and openly being exploited. It is a difficult balance.

Of course, you have to be careful not to take a blunt approach to some of the adult service websites that operate, technically legally, at the moment. I would argue that they are not legitimate. There is always a risk of displacement for some women to on-street activities where the risk factors might be greater. We need to be very conscious of that. My point is that there are a number of these sites with tens of thousands of adverts. If you were to type "company of young girls", on three main websites, you would find hundreds and hundreds of adverts. It is on a deeply worrying scale. They are used to traffic vulnerable young girls across the United Kingdom at the moment, principally but not exclusively from eastern Europe. We should be deeply concerned about that, and those technically legal platforms are facilitating it.

Detective Superintendent Phil Tomlinson: We have some evidence-based experience in counterterrorism that relates to the point about whether it drives activity to other areas. It is fair to say that some of the big US companies were bashed up in the media about 12 months ago because of extremist material appearing on their platforms. Those companies have worked really hard and removed a lot of that content. There have been influences that reduced the amount of extremist material online because of what is happening outside the UK, but we have seen a shift of terrorist material to other more secure platforms.

It comes back to whack-a-mole. There is no doubt that, if you start going after one company, it pops up in more secure areas, which are harder for us to reach. It is harder for us to engage with those companies, which are often based in harder-to-reach countries. Without doubt, we have to bear in mind the impact of pushing activity away from the big companies, where there are benefits in being able to see what people are doing, to more secure sites where potentially you do not see what is going on. It has an impact on the circulation of videos, but it also potentially impacts

on your ability to see what they are doing and the methods they are employing to use propaganda, et cetera.

Q43 **Viscount Colville of Culross:** Mr Toon and Detective Superintendent Tomlinson, you have talked about the importance of international co-operation between police forces, law enforcement agencies and international stakeholders. Are there problems that we need to overcome to make sure that that co-operation is ever stronger and more intense? There is a great difference in the approach to freedom of expression between America and the EU, for instance, and I would like you to address that. The second part of the question is: does the prospect of Brexit pose a problem for international co-operation between our country and the EU?

Detective Superintendent Phil Tomlinson: International collaboration is crucial. We talked about the fact that this is a global issue, not just a UK one. The internet referral unit has set up a process, a model, that works very well in the UK, and it has been replicated in a number of countries around the world. We work very closely with the EU Internet Referral Unit, where we have staff working to ensure that across Europe everyone has the same sort of process and benefits that we have developed in the UK.

We work closely with the other Five Eyes countries and internationally to educate and inform them about the benefits we have experienced in the UK. We have had some significant benefits in relation to CT in the collaboration we have had. We also work very closely with the Home Office to develop international reach with companies overseas. Working internationally is absolutely crucial to our effort.

We are fortunate in the UK that we are a bit ahead of the curve in respect of our engagement, and that is a model now being copied by other countries. We have regular visits from and meetings with our European and international partners to discuss ways of working, to make sure that everyone is working in the same way.

Mr Donald Toon: From a wider criminality perspective, the system and the underlying tools are there; they are effective and are absolutely critical for us to work effectively together. They are not necessarily specific. For example, on the cybercrime side, the European Cybercrime Centre in Europol is hugely important to our ability to operate effectively, but it is not bound by the EU itself, so it is not a Brexit-related issue. The fact is that the second largest bureau in Europol is that of the United States.

There is a very strong and capable approach in being able to engage a range of different partners. We use that alongside the Five Eyes structure on a standard basis to co-ordinate our activity in a wider range of countries. We have used it particularly on economic and cybercrime in the countries of south Asia and the far east of Europe to have an effective response and share both intelligence and evidential material. The

systems and tools are effective. Fundamentally, the issue becomes one of will, and the desire to use them effectively.

Viscount Colville of Culross: Do you think Brexit poses a threat to that?

Mr Donald Toon: It is hard to see that Brexit in itself poses a direct risk. The fundamental issue is that, beyond Europe, we have very effective tools. What is important in the Brexit context is that we are able to continue to work effectively on joint action to investigate and arrest. There will be issues around the ability to be effective with partners within Europe. Capabilities such as the use of European investigation orders and European arrest warrants remain important to us. It is important that through Brexit we do not lose the ability to take action against criminals operating from Europe and affecting the UK, or UK criminals operating from elsewhere in Europe. It is important that we do not lose those capabilities through Brexit. That is fundamentally the issue around Brexit, rather than international co-operation in the round.

The Chairman: Do any of the other witnesses have concerns about Brexit?

Chief Constable Stephen Kavanagh: Donald has expressed it clearly. If there is anything that undermines our ability to produce orders or have arrest powers with our closest partners, we would need to tread carefully.

Lord Allen of Kensington: Are there any countries ahead of us from which we can learn from a legislative or regulatory perspective? Germany is a potential area; we have had input from Australia. With your international network, who is ahead of the game? If they are, what is the particular area?

Mr Donald Toon: The short answer is that there is not necessarily anyone ahead of the game. There are strengths and weaknesses in the approaches of most countries. A lot of approaches are very much tailored to the circumstances of the individual country. It is often much easier to operate and have more effective control if you are in a relatively small and tightly defined jurisdiction. What really matters is the ability to co-ordinate, collaborate and co-operate effectively.

I would not say there is any shining light to which we should all be aspiring. The truth is that the vast majority of jurisdictions are facing very similar problems and trying to grapple with them and find a way forward. The real issue is making sure that we can support each other, and that we recognise that this is a worldwide problem. We have to be able to have impact, engagement and understanding in all affected jurisdictions. We cannot do this alone.

The Chairman: I thank our witnesses very sincerely for their evidence, and for giving us so much time and being so comprehensive. Susie Hargreaves, you sent us some written evidence as well, which we appreciate. Two hours have gone very quickly, and there may be other

issues you would have liked to draw to the attention of the Committee. If so, please do not hesitate to write to us with further evidence, or reading, that you think we might find useful.

Our witnesses work in some dark and disturbing areas. I am struck by the humanity that you bring to your work and the approach you take. I thank you on behalf of the Committee for all the work you do and the service you give, as well as for giving us evidence today. Thank you.