

APPG on
Social Media



All- Party Parliamentary Group for Social Media Meeting
Law Enforcement Session as part of “Selfie Generation” Inquiry
Wednesday 19 May 2021

Attendees:

Chris Elmore MP, Chair of APPG on Social Media
David Linden MP, Vice-Chair APPG on Social Media
John Nicholson MP, SNP Shadow Culture Secretary
Lord Stevenson
Baroness Lynne Featherstone
Rachel Edwards, Office of Maria Miller MP
Alexandra Landes, Office of Chris Elmore MP
Nansi Morgan, Office of David Linden MP
Sabah Kanwal, Office of Debbie Abrahams MP
Christopher, Office of Catherine McKinnell MP
Lucy Cserna, Office of Sarah Champion MP
Frances Lasok, Office of Saqib Bhatti MP
Joe Hamblin, Office of Siobhan Ballie MP
Nasra Elliott, Office of Kim Johnson MP
Tony Stower, 5Rights and Office of Baroness Kidron
John Carr
Sarah Gregory, National Crime Agency
Tim Wright, National Crime Agency
Hannah Small, Children’s Society

Speakers:

Rob Jones, National Crime Agency
Chief Constable Simon Bailey, National Police Chiefs’ Council lead for Child Protection
Tom Squire, Lucy Faithful Foundation

Secretariat:

Michael Tunks, Internet Watch Foundation and UK Safer Internet Centre
Abigail Fedorovsky, Internet Watch Foundation and UK Safer Internet Centre

Apologies:

Maria Miller MP
Catherine McKinnell MP
Baroness Karren Brady
Lisa Cameron MP
Damian Hinds MP
Bambos Charalambous MP
Aaron Bell MP
Sarah Dines MP
Lord Taylor of Warwick
Baroness Newlove
Lord Blunkett
Baroness Ritchie of Downpatrick
Lord Foulkes
Stephen Timms MP
Baroness Hamwee

1. Opening remarks- Chris Elmore MP

Chris Elmore opened the session and welcomed those giving evidence. He also passed on his thanks to David Linden, who kindly agreed to take over Chairing the session halfway through and facilitate the Q&A session as Chris had to attend another meeting.

2. Opening remarks from Panel Members-

Rob Jones:

Rob opened by explaining the operational context law enforcement is currently operating within. Rob outlined that the scale, severity, and nature of the threat have all increased.

Last year the NCA's annual threat assessment estimated that 300,000 people in the UK posed a threat to children either through offline or online offending.

A new assessment is currently being prepared, where it is anticipated that those numbers will grow further.

In terms of self-generated indecent images, these can be obtained through coercion or come from consensual image sharing.

There is a clear link between the prevalence of these images and offending.

The NCA is concerned about the extremely low bar to offending on the open web and that mainstream search engines are regularly returning Category A images within three clicks.

There is a cycle of incitement to create new images.

Rob went on to outline a recent investigation into David Wilson which has recently concluded. Wilson masqueraded behind 20 different Facebook accounts as a young girl, and he managed to contact 5,000 children and 500 of them were enticed into sharing images of themselves. Most of those victims were boys. Wilson then incited the children into abusing their siblings or friends, and then threatened to reveal those images.

This type of case is extremely difficult to deal with and there are many others like him. It took NCA four years to build the case against him and he was eventually found guilty of 96 offences and sentenced to 25 years in prison.

There are many other cases that the NCA deal with where one person is able to victimise hundreds of children using the internet.

The case also highlights how industry can assist law enforcement. Facebook were very helpful in this case by providing cyber tip reports which assisted the NCA's investigation.

The NCA remain concerned about Facebook's future business plans. The NCA have been trying to gain commitment from Facebook that cases such as David Wilson will continue to be identified if Facebook encrypts its messenger service and so far, that assurance has not been forthcoming.

If you compare the number of referrals from WhatsApp which is end to end encrypted, you will see that they account for very few reports to the National Centre for Missing and Exploited Children (NCMEC).

In terms of the response, we need to deal with prolific offenders; we need to reduce the demand for imagery, and we need to ensure that children are also well equipped to respond to break the model of extortion. If a child is able to seek help from a parent or carer, this can stop the cycle immediately. The NCA have an education team and are releasing a campaign soon which takes children and parents through scenarios that teaches them to make good decisions when it comes to this issue.

We have got very good at locking people up, but the low bar to entry on the internet makes this very difficult to respond to currently.

Simon Bailey:

Tackling Child Sexual abuse remains a national priority. We have invested significant national, regional, and local resources to addressing this problem.

At the Pursue Board every month we hear updates on how many people we have arrested and how many children we have safeguarded. We have arrested 7,000 people in the last year and safeguarded 10,000 children.

This is a world-leading response, but the number of referrals continue to grow and grow. A large part of this is due to the rise in selfies or self-generated content.

The 1978 and 1988 laws which creates the offence of making and sharing indecent images were not designed for the current digital age. It doesn't give children confidence in the law and currently doesn't differentiate the differences between the involvement of an adult and a child.

Taking and sharing of indecent images takes place in different ways; consensual in a relationship to being groomed and extorted. What can start with consensual image sharing can very quickly become non-consensual and can be rapidly shared online.

It will come as no surprise that Facebook are responsible for the vast number of referrals law enforcement.

Law Enforcement have gone to great lengths not to criminalise children for sharing images. College of Policing advice issued in 2016, sought to ensure children were not inappropriately criminalised. But in doing so, we must also ensure that we work with Home Office to record crimes correctly and accurately.

Ofcom has recently produced research which helpfully details children's use of social media platforms. That research has also found that their usage has increased during the period of lockdowns- inevitably this will lead to a far greater number of referrals.

There is a concerning number of children who are doing this and the figures from the IWF back up this suggestion.

There is some research which suggests there are also long-term health and mental health implications in the sharing of this imagery. Children never imagine the implications of sharing this imagery, how it is shared online and how paedophiles may use their imagery.

Advice from the College of Policing states the primary focus must be working on supporting the welfare of children and there is a need to work in schools. The recent Everyone's Invited movement has demonstrated the importance of this.

Working with the Home Office to create Outcome 21, gives us the ability to shut down an investigation because it is not in the public interest to pursue an investigation because it has been established that a child created the image. We then must work with the Disclosure and Barring Service (DBS) to ensure that this does not adversely affect the life chances of children and young people in securing work in the future.

The College of Policing's advice is subject to review and that review will be published soon and that work will be shared with this group.

Challenges remain around consistent interventions of wider inappropriate sexual behaviour, particularly for teachers. Teachers feel particularly out of their depth when it comes to dealing with these issues as part of the "selfie-generation".

The Strategic Assessment is due to be published shortly and inevitably this will demonstrate a further increase in addressing this issue. Too many of these self-generated images are finding their way onto the web and law enforcement are then responsible for dealing with the fallout.

Tom Squire:

The Lucy Faithful Foundation is a child protection charity established in 1992 focussed on the prevention of child sexual abuse and exploitation.

It is our view that we need a range of approaches and interventions to address this issue. It is the responsibility of all of us to address this issue.

As the Home Office Tackling Child Sexual Abuse and Exploitation strategy sets out, we must safeguard children and encourage them to report any incidents.

The online environment needs to be fit for purpose.

We need to detect and prosecute those that have abused children.

We also need to reach out to those who might be tempted to; or have crossed the line in abusing children, and we can help them to address the reasons why.

This is critical because of the scale of the problem. We cannot simply arrest our way out of this problem.

At Lucy Faithful we set up the Stop It Now helpline in 2002 and now deal with 1,400 contacts per month from around 800 individuals. 50% of those are directly concerned about their online behaviour and 1 in 5 have solicited indecent images from a minor. The majority call about viewing indecent images, but some call regarding their behaviour to do with online grooming.

The Foundation has also been a victim of its own success. Demand for its services is currently outstripping supply and whilst the Foundation dealt with 1,000 calls every month it is currently missing 2,000 per month in the previous financial year.

We helped 7,000 people in the last year, but sadly we missed helping around 2,000 more.

We have developed an online chat service and online self-help guides. Over 170,000 people have clicked through to these self-help services. Both things have helped to increase our reach.

Importantly, independent evaluations have shown that a number of these people have changed their behaviours as a result.

Question and Answer session:

David Linden thanked the panellists for their contributions citing the scale of the problem as particularly stark and then introduced the Q&A session.

David asked a question about how we encourage children to make better, more informed choices?

Simon Bailey: It must start at home with parents having a conversation with their child about what they can expect from the online world. Schools then have a huge role to play around misogyny and inappropriate sexual behaviour. We also need to have a conversation about the impact of pornography on the ability of children to develop healthy relationships. We then need to use online platforms to target 11–13-year-olds using social media influences and others to target children to reinforce that message in the way the IWF are currently doing.

Rob Jones: These outreach programmes must be credible. But we must also enable parents to give them the tools to have these conversations. We also need to make it much more difficult for this content to be found online- particularly through search engines. If children progress in the wrong way in their browsing of adult pornography, they will end up viewing child sexual abuse imagery. If it is so easy for children to view pornography, this risks undermining messages from parents and schools about what healthy relationships look like.

John Nicholson: This is a generational challenge, the thought of some of this takes my breath away. The DCMS Select Committee are looking at the role influencers play, are social media companies doing enough? The APPG on Media Literacy heard concerning evidence of adults encouraging children to do some extremely dangerous things, yesterday, we heard evidence directly from children about this. Hashtags often direct people to these sorts of content.

Is legislation and effective, I fear the only way of holding them to account is through fines and penalties- because it has worked in Germany. What more can the companies do?

Secondly, as a journalist, I did some research into the profile of abusers. It is very difficult to “cure” those with these tendencies. Even with very intense social work interventions. How do we get that right in the context of the Internet- perhaps Tom might pick this up?

Simon Bailey: I was quoted in a national newspaper recently about the fact that Registered Sex Offenders were using Instagram profiles. A newspaper discovered 100 registered sex offenders using the platform. If this were a shop on the high street, it wouldn't be possible for 100 sex offenders to gather at a store where children are.

It is my opinion that the only way of addressing this is through legislation and it is simply taking too long. My concern is that due to the numbers we have placed before you that many more children will be abused before the legislation is enacted.

The companies want me to provide a list to them of all the registered sex offenders. We can't do that, but if the Daily Telegraph can find these offenders, then why can't they do something about that?

We are also really concerned about Facebook turning the lights out on our ability to detect CSAM due to their stance on encryption.

In 1990, a Home Office estimated there were 7,000 images in circulation. Today, the Child Abuse Image Database has 17 million unique images within it- that gives you further evidence of the impact the internet has had on this activity.

Rob Jones: The companies are not doing enough. There is a torrent of images which are detectable with technology being available to offenders. That cannot be right. The technical expertise they have and some of the problems they solve for the pursuit of profit, daily, demonstrates the companies could solve this. They have the data and know the most about how their platforms operate. We shouldn't have to legislate for them to do something about this, they could start doing this now.

Tom Squire: Agree with the other witness that companies can do more. On offending profiles, they are a mixed group, the starting points and their progression differs and that therefore influences the advice we give. This is important to understand as it informs the interventions needed.

Some people are highly sexualised and contact many children at the same time. With others it is a much slower burn. They find children easier to talk to and it is a longer engagement process before they then request sexual imagery.

Some may know the children through the offline world but use pseudonyms through the online world to exploit the children that they know.

Rachel Edwards: Maria Miller is interested in the law enforcement response to sexting on a peer-to-peer basis. Many children don't know this is illegal, is this communicated in advice and guidance to schools?

Frances Lasok: What are the differences between the social media companies in their response to this issue?

Rob Jones: Simon has provided details on Outcome 21, so I will leave that to him. Facebook has 2.2bn unique users, there are children masquerading as adults, adults masquerading as children. From a standing start, there is no other platform with that level of reach. What they are doing now, in terms of the visibility of the platform is good, but we are very concerned about the impact of encryption. Whatsapp is very different because it has been encrypted since 2014; it is therefore responsible for lower-level referrals to the National Centre in the United States.

Other platforms have the same functionality to a varying degree. The platforms should be taking greater steps to age verify their users. The Duty of Care established by the Online Safety Bill regime is something we should also hold onto when considering private spaces.

Simon Bailey: Children are aware that they are breaking the law, but society has moved on and children know that they are breaking the law, but we perhaps need to look at this issue much more closely.

David Linden: Thanked everyone for their questions and contributions and passed over to Mike to wrap up on the next steps before closing the session.