Criminal Justice Committee

16th Meeting, 2022 (Session 6), Wednesday 18 May 2022

Online child abuse, grooming and exploitation

Note by the clerk

Introduction

1. The Committee is to hold a roundtable evidence session on online child abuse, grooming and exploitation on 18 May 2022.

2. The evidence session will focus on the measures being taken, and those necessary, to tackle online child sexual abuse, grooming and exploitation.

Participants

3. The Committee will hear from:

- Stuart Allardyce, Director Stop It Now! Scotland, Lucy Faithfull Foundation;
- Alison Penman, Child Protection Sub Group, Social Work Scotland;
- Joanne Smith, Policy and Public Affairs Manager, NSPCC Scotland;
- Gina Wilson, Head of Strategy, The Children and Young People's Commissioner Scotland;
- Assistant Chief Constable Bex Smith, Major Crime, Public Protection and Local Crime, Police Scotland; and
- Miles Bonfield, Deputy Director Investigations North, National Crime Agency.

Format

4. Members of the Committee and witnesses will be attending the meeting in person for this roundtable evidence session.

5. The Committee received written evidence in advance of the session, which can be accessed at Annex A.

Clerks to the Committee
May 2022

Annex A – written submissions

Stop It Now! Scotland

Introduction: Stop It Now! Scotland

Stop It Now! Scotland is part of the Lucy Faithfull Foundation, the only UK charity focused exclusively on the prevention of child sexual abuse. We work with adults who are worried about their own sexual thoughts, feelings or actions towards children and who cannot access statutory supports from services such as health or criminal justice social work.

Our Edinburgh based team works across Scotland – we provide services both face to face and online. All our staff have a child protection background coming from professions such as social work, law enforcement, education and forensic psychology.

We work with people who have been arrested for online sexual offences against children including viewing indecent images of children / child sexual abuse material. The vast majority of those we work with self-refer after being provided with information about our services by Police Scotland when they are arrested for an online offence. In 2021-22 we worked with 99 people**.**

We also support family members of those who have been arrested. Many of them are wives and partners, but also parents whose adult sons have been charged with an online offence. Families are often devastated by the arrest of a loved one and research suggests that around 70% of family members who have experienced “the knock” from the police arresting a loved one go onto experience severe post-traumatic stress disorder (PTSD). We provide a ‘safe place’ for family members to start to understand the offending behaviour, to talk openly about the issues following on from the arrest of a loved one and gain support in protecting any child that may be at risk. In 2021-22 71 family members referred themselves to our service for support.

We also take the learning from our work with adults who pose a sexual risk to children and translate it into resources for parents, professionals and the general public that promote evidence-based prevention of sexual abuse before it occurs.

A Public Health Approach to Child Sexual Abuse

Stop It Now! Scotland’s approach to child sexual abuse prevention is predicated on there being an understanding that child sexual abuse is a public health issue and that there are steps that every adult can take to make Scotland a safer place for children to grow up.

Scotland has a chance to change the way it approaches online child sexual abuse prevention. Criminal justice responses to sexual offending and child sexual abuse are critically important: we have to bring offenders to justice and must ensure the needs of victims are at the heart of our judicial system. But if our only frame of reference for tackling child sexual abuse continues to be through the criminal justice system then we miss an opportunity to **prevent** abuse rather than "just" responding to it.

We urgently need to think about this problem beyond one of law enforcement and shift 'upstream', investing in preventing sexual abuse before it happens.

This allows a shift from professional-led responses after abuse is identified to engaging with communities as active partners in finding the solutions to this issue before it happens. This involves a pivot towards prevention and early-intervention involving three key steps.

- Raising awareness of online child sexual abuse

Offenders can be deterred when people talk about child sexual abuse openly and know that supports are there for people before harm is caused. If no one is talking about safety and protection, then it is easier for potential offenders to rationalise thoughts, feelings and behaviours that will lead to harm and they lack signposting to services and resources that can prevent abuse before it happens.

- Deterrence and disruption of those who present a risk to children.

Since 2018 we have worked with Police Scotland to deter online viewing and sharing of sexual images of children and online grooming using press coverage, digital adverts and partnerships to spread key messages. The aim is to disrupt and deter potential offenders and provide early help for those at the cusp of online offending to promote the prevention of online child sexual abuse and exploitation. The deterrence campaign in 2021 contributed to over 2000 people in Scotland accessing our Get Help online resources for adults who are worried about their viewing of sexual images of children online and want to seek help to stop. This work tells us that a proportion of online offenders will seek anonymised help to desist from offending behaviour before arrest if they are aware that support exists.

- Reducing opportunities to offend

This involves engagement with tech companies to ensure that safety by design is promoted and platforms focus on how the internet needs to be re-built around the needs of our children. Under 18s represent 1 in 3 internet users globally.

A significant development this year was the Lucy Faithfull Foundation pro-bono work with MindGeek, owner of adult pornography websites including Pornhub. MindGeek had already recognised attempts by a small minority of users to seek child sexual abuse material using banned search terms. Following our collaboration, these searchers now receive a clear message about the illegality of sexual images of under 18s; the harm done to victims; and about the help available to stop through our confidential helpline and Get Help self-help resources. Between the launch in early

February 2021 and 31 March 2021, nearly 22,000 users from around the world clicked through to our website after seeing a deterrence message. This builds on similar work we have undertaken with Google and other tech companies.

All of this needs to be locked into a clear action plan or strategy in Scotland so that services and initiatives are co-ordinated, evidence based and resources and investment have maximum impact.

What is currently defined as online child sexual abuse?

The 2021 National Guidance for Child Protection in Scotland states simply that:

"*Online child abuse is any type of abuse that occurs in the digital environment and the internet, facilitated through technology and devices such as computers, tablets, mobile phones, gaming devices and other online-enabled devices*."

In January 2016, the Interagency Working Group on Sexual Exploitation of Children in Luxembourg adopted ECPAT International's 'Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse'[2]. The guidelines were developed in recognition of the significant challenges for policy development and programming, development of legislation, and data collection when there is still considerable confusion surrounding the use of different terminology related to the sexual exploitation and sexual abuse of children. However ECPAT's definition of online child sexual abuse recognises:

"*…sexual exploitation and sexual abuse of children increasingly take place through the Internet, or with some connection to the online environment. Online sexual abuse can be any form of sexual abuse of children… which has a link to the online environment. Thus, online sexual abuse can take the form of, for instance, sexual molestation and/or harassment through social media or other online channels. Child sexual abuse also takes on an online dimension when, for instance, acts of sexual abuse are photographed or video-/audio-recorded and then uploaded and made available online, whether for personal use or for sharing with others…Each repeated viewing and/or sharing of such recorded material constitutes a new violation of the rights of the child….It is important to note, however, that online child sexual abuse is not, in and by itself, a new and distinct form of sexual abuse. Rather, different manifestations of child sexual abuse are facilitated by the Internet, and can increase the accessibility to children by persons looking to sexually abuse them.*".

What is the scale and extent of this crime?

In 2021, 361,062 reports of child sexual abuse imagery were assessed by the Internet Watch Foundation (+20% from 2020). 252,194 URLs were confirmed as containing child sexual abuse imagery, having links to the imagery, or advertising it (64%+ from 2020).

The 2021 threat assessment from the National Crime Agency reported that there are between 550,000 and 850,000 UK based individuals who pose various degrees of sexual risk to children. The figure combines those currently on the sex offender register and a much larger figure of individuals whose online behaviour suggests they present a risk of harm to children, including viewing indecent images of children.

There are some indicators that issues around online harm have been aggravated by COVID lockdowns. The Lucy Faithfull Foundation saw an 11% increase in people contacting our Stop It Now! Helpline from 2019 to 2020, alongside a 42% increase in views of our Get Help user introduction page for adults worried about their online behaviour. Additionally, the NSPCC recorded a 60% average monthly increase in contacts made about children experiencing online child sexual abuse- during/post the first national lockdown, compared to pre-lockdown figures.

In 2021, the WeProtect Global Alliance Threat Assessment reported that 1 in 3 (34%) respondents to their Economist Impact global survey were asked to do something sexually explicit they were uncomfortable with during childhood. They also reported that the Internet Watch Foundation saw a 77% rise in child 'self-generated' sexual material from 2019 to 2020.

In short, the nature and scale off online sexual abuse is so massive that it is impossible to arrest our way out of this problem. Law enforcement needs to focus on those who presented the greatest threat to children and prevention and early help services have a considerable role to play in tackling this issue within a broad, public health orientated prevention framework.

How agencies and organisations are responding and what are the challenges?

The key challenge for all agencies in Scotland at present is the lack of an overarching strategy to tackle online child sexual abuse. Scotland has a wealth of services working within this area but there is no government leadership with the issue straddling multiple government departments and Ministerial portfolios. Any strategy would have to consider a continuum stretching from prevention, deterrence and early help through to conviction and rehabilitation. The UK Government and the Welsh Government have both published strategies to tackle child sexual abuse in the last few years featuring sections on online harm with the Welsh Government producing a standalone action plan specifically addressing online harm
Demand for services also continues to grow as awareness of online sexual abuse grows. Additional resourcing would be needed to scale work necessary to have maximum impact in this area.

Stop It Now! Scotland contributes significantly to the response to online sexual harm across the country and we are the only charity working with adults who pose a sexual risk to children online.

We run a range of services including:

  - **Inform Plus** – for men who have viewed illegal images of children online, suitable for those who are pre- conviction. At present it takes around 2 years for online offenders to be convicted, and suicide risk amongst arrested but unconvicted online offenders is extremely high in comparison to individuals who have no contact with the criminal justice system. This ten-week psychoeducational group work programme allows the right supports to be targeted at the right individuals at the right time. Individuals can self-refer to access this group work programme. The programme covers key areas such as relapse prevention, the criminal justice system and the impact of online offending on children themselves.

  - **Breaking the Links** – An adaptation of Inform Plus for individuals who have been involved with online offending who have a history of trauma in their own background. Data from 800 individuals we have worked with since 2011 at Stop It Now! Scotland reveals that 12% of those who self-refer have themselves experienced sexual abuse in childhood – around 3 x the expected rate for men in Scotland.

  - **Engage Plus** – A 1-1 programme men who have who have engaged in sexual conversations with children online.

  - **Inform Young People** – A 1-1 psychoeducational programme for young people and young adults who have displayed sexually abusive behaviour online. It is suitable for children aged 13+.

  - **Inform** – for family members or friends of people who have offended online. Families are not traditionally seen as victims of such offending, even though they are often left devastated by the actions of a loved one. Inform offers a safe space in which people who are struggling with the emotional and practical impactof internet offending can bring their questions and anxieties and begin to explore them in a supportive environment. This year we worked with a total of 71 family members either in person (remotely), or over the phone. 95% of participants who completed Inform courses said they felt less isolated after the programme. We also provide direct service for children affected by arrest of a parent.

- **Helpline**: The Stop It Now! UK and Ireland helpline is the largest child sexual abuse prevention helpline in the world. Run by our parent charity, the Lucy Faithfull Foundation, this unique service is available for anyone with any concern about child sexual abuse. The service is confidential and anonymous. Callers range from those concerned about their own sexual thoughts or behaviour towards children to those concerned about the sexual behaviour of another adult, child or young person; to professionals seeking case advice to adult survivors of child sexual abuse. The helpline provides far more than simply a listening service. We provide callers with practical, real-life advice and actions that they can take to keep children safe. In 2020/21 across the UK we helped 7,300 people who between them made 14,197 contacts (calls, chats and secure messages). This is a significant increase on callers (5,959) and contacts (10,636) in 2019/20. Stop It Now! Scotland receives referrals directly from the helpline.

Protecting children from sexual content online and on social media

Children's online safety requires a multi-layered, systemic approach, involving legislators and regulators, law enforcement agencies, social media and website owners, schools, parents, and children and young people themselves. In December 2021, we joined with other child protection charities in a campaign led by Barnardos. We signed an open letter to the owners of the most-viewed pornography websites in the UK, calling on them to prevent children from accessing their sites by implementing age verification as soon as possible, and to remove illegal and harmful content from their platforms.

Launched in 2019, our Upstream online resource gives information, support and advice to families who want to know more about how to keep children and young people safe from sexual abuse online. This resource turns the learning from our work with those who pose a risk to children into vital information to engage parents and other protective adults giving them the knowledge, skills and confidence to help their children stay safe online.

In 2021 and 2022 we worked with the Scottish Government's cyber resilience unit to develop a training programme for kinship carers, foster carers, adoptive parents and the social workers who support them on digital resilience and online safety. The programme was significantly over subscribed and has been delivered to over 200 carers and social workers across Scotland to date.

Educating young people about online abuse, grooming and exploitation

Teachers and parents should know what constitutes healthy and expected sexual behaviour at different ages of childhood and adolescence so that they can teach healthy boundaries and know when to be concerned – and what to do with relationship concerns. The February 2022 Parent Club campaign on child online safety is a good example of campaign work in this area targeting parents. Messaging needs to ensure that parents have basic knowledge about online safety and where they can get advice. However the heart of online safety needs to be parents having a proactive interest in their child's online lives and the provision of age appropriate monitoring, supervision and gate keeping.

Promoting key messages to children about consent needs to be at the heart of prevention of all kinds of sexual abuse and exploitation, including online abuse. Sometimes online safety is presented as a separate issue from sexual violence prevention, but this is an artificial distinction. Successful schools-based activities look at what trust and consent means in a relationship, and practice skills including how to respond to solicitations, both online and offline. Young people need opportunities to share their views around what consent is, to explore values, and to discuss relationships. Education can help them to distinguish when someone really cares about them from when someone is being sexually exploitative. Discussions about sexual risk taking online and offline should take place in a context of children's rights, underlining children and young people's rights to make choices, models of consent and also emphasising the responsibilities of adults to help protect young people from harm.

Appropriate curriculum materials can be found at https://rshp.scot but more specialist support and training is needed for education staff to address this issue. A significant proportion of online harm is caused by children and young people themselves, through non-consensual sharing of self-produced sexual images, sexual harassment online etc. We have worked with Education Scotland developing resources for schools on tackling this issue, but further support to schools is needed to ensure that their approach to online abuse prevention is evidence based and grounded in best practice.

Providing support for children to recognise they are being abused, groomed or exploited

Our expertise is in working with adults to keep children safe from sexual harm. We believe it is the responsibility of adults to keep children safe. However we recognise the vital work of others in providing support for children and young people to recognise if they are being abused, groomed or exploited and we stay up-to-date with the best resources and services that other agencies offer in order to signpost children and young people effectively.

In March 2022, the National Crime Agency's CEOP Education Team launched a new website for professionals, parents/carers and children and young people aged 4 to 18 years old. The section for children and young people is divided into three separate sites for 4 – 7, 8 - 10 and 11 – 18 year olds with age-appropriate content on sex, relationships and the internet.

We also inform professionals, parents, children and young people about useful tools, such as the NSPCC and IWF's 'Report Remove' tool which allows young people to report an image or video shared online, to see if it's possible to get it taken down. It keeps the young person informed at each stage of their report, and provides further support where necessary. We would like to see the promotion of such tools more proactively across Scotland.

Final thoughts

Scotland has the chance to change the way it approaches the prevention of child sexual abuse online if there is enough political will. There are three ways that a real difference to prevention could be made in a relatively short period of time. These are:

1. The development of a Scotland-wide strategy to tackle online child sexual abuse. The strategy would focus on the true prevention of abuse looking not only at who the victims are and how to support them, but addressing offender behaviour and examining pathways into offending and how potential offenders can be disrupted to prevent abuse from occurring at all.

2. Urgently investing in support for families affected by the arrest of a loved one and acknowledging that families are secondary victims of child sexual abuse.
3. The commitment to the continuation of deterrence campaigning across Scotland aimed at deterring and disrupting potential online offenders before they commit harm.

We look forward to discussing these issues with you in person.

Barnardo's Scotland

This document is a brief summary of Barnardo's Scotland activity and experience on tackling online child abuse, grooming and exploitation and we have chosen to focus our remarks around the context of the Online Safety Bill currently progressing through UK Parliament.

Introduction to Barnardo's Scotland services and campaigning

Since the early 1990s, Barnardo's Scotland has been tackling child sexual exploitation and abuse in Scotland, supporting victims, raising awareness in communities, and calling for national leadership.

In 2012 the Scottish Parliament's Petitions Committee showed cross-party political leadership when it supported a petition submitted by Barnardo's Scotland to highlight child sexual exploitation and improve our response to the issue. Sadly we know that children in every community are still at risk from this horrific crime. The exploitation and abuse of vulnerable young people is one of the most serious child protection issues of our time; however the true scale of the issue remains largely unknown.

There remains the need for improved identification of child exploitation and abuse; appropriate supports for its young victims, and the collection and collation of data on the prevalence, nature and scope of child exploitation and abuse in Scotland. Barnardo's delivers support services in Dundee, Edinburgh, Glasgow and the West of Scotland and we know that more needs to be done to shift the national narrative from just treatment to early intervention and preventing child exploitation and abuse from happening in the first place. As the world changes and evolves so do the risks facing young people. We know all children can become victims of sexual abuse and exploitation: girls and boys, from every ethnicity, religion and cultural background; LGBTI young people; and those with disabilities. Children who have already experienced neglect and abuse are especially vulnerable, but with new technologies all children are at risk of being groomed online, often by adult predators using the cover of anonymity to exploit them.

Scale and extent of this crime

Barnardo's Scotland produced a report in collaboration with the Scottish Children's Reporter's Administration in 2020 on the scale and nature of child sexual exploitation of children and young people involved in the children's hearing system.

Our research found evidence of exploitation in 27 of Scotland's 32 local authority areas and produced 15 recommendations for action, including asks on the Scottish Government to invest in fresh research into the issue of CSE and in public awareness campaigns. Has agreed that

Protecting children from sexual content online and on social media

Barnardo's is currently campaigning to strengthen and improve the Online Safety Bill, currently under consideration by the UK Parliament, to make the internet a safer place for children and young people.

The Online Safety Bill is a vital opportunity to protect children from a wide range of harms online.

Pornography

Viewing pornography – often extreme and violent – distorts children's understanding of healthy relationships and can normalise abusive sexual behaviour.
So far we are pleased that the UK Government has listened to the views of Barnardo's and other experts and has agreed that age verification is needed for commercial pornography sites.

We are concerned however, that these provisions could take more than three years to implement with children accessing pornography millions more times in the meantime causing untold harm.

We are also concerned about illegal content on commercial pornography sites as well as content that is harmful but legal. Content is freely available that would not be permissible or legal to view offline by the British Board of Film Classification (BBFC) who regulate offline pornographic DVDs. Content depicting abuse, violence and incest. There is also a huge amount of animated pornography available which uses children's favourite TV and film characters to entice them to watch. Although much of this content is illegal, there is a lack of enforcement from the sites in removing it. There is also a large amount which is not considered illegal such as adults dressing as schoolgirls or sexual relations between older men and young women but is extremely harmful and would not be permitted offline by the BBFC. As the Bill stands commercial pornography sites will not be required to remove harmful material.

Criminal Exploitation

We welcome the proposed 'duty of care' on social media companies contained in the Online Safety Bill as it stands, and some other platforms that allow users to share and post material, to remove 'harmful content'. This duty rightly includes content that is legal but harmful to users, including children.

However, the Bill does not cover another form of abuse: child criminal exploitation. This is where a child is manipulated or coerced into undertaking criminal activity. It often takes months or longer for criminal exploitation to be identified, and sometimes the child is criminalised.

The UK Online Safety Bill is an opportunity to strengthen legislation on online grooming for the purpose of children criminal exploitation and also provides an opportunity for the Scottish Parliament to consider how we tackle this issue in the Scotland context.

Internet Watch Foundation

1. About the Internet Watch Foundation

1.1. The IWF is a UK charity that works in partnership with the internet industry, law enforcement and government to remove from the internet (with the co-operation of industry) child sexual abuse images and videos wherever they are hosted in the world and non-photographic images[1] of child sexual abuse hosted in the UK.

1.2. In addition, the IWF has established reporting portals – places to report online child sexual abuse imagery anonymously and safely – in 49 countries around the world, serving 2.5 billion people.

1.3. There is a Memorandum of Understanding between the National Police Chiefs' Council (NPCC) and Crown Prosecution Service (CPS) that governs our operations. This ensures immunity from prosecution for our analysts and recognises our role as the "appropriate authority" for the issuing of Takedown Notices in the UK. Operationally, we are independent of UK Government and law enforcement but work closely with both.

1.4. The IWF also plays a vital role in providing the internet industry with several quality-assured technical services to prevent the spread of known child sexual abuse images and videos online and to stop the upload of images in the first place. These include image hashing utilising Microsoft's PhotoDNA, a URL blocking list of live webpages, keywords list, domain alerts, payment brand alerts, newsgroup alerts and simultaneous alerts (for US companies only). Key to this is our trusted relationship with the internet industry which enables us to act as a broker between them, and government and law enforcement.

1.5. Our work is funded almost entirely by the internet industry: 90% of our funding comes from our members with the remaining 10% of our funding applying to our role as part of the UK Safer Internet Centre, coming from Nominet, who are a world leading domain name registry based in the UK and responsible for administering the .UK domain.

1.6. The IWF has previously received additional Government funding for specific projects and is open to further diversifying its funding mix in the future.

1.7. We are a charity registered in England & Wales with an 11-person Board of Trustees of which, eight are independent members and three are industry

[1] Non-Photographic Images include cartoons, drawings, computer generated imagery (CGI) and other non-photographic depictions of child sexual abuse that are deemed to have breached sections 62-69 of the Coroners and Justice Act (2009).

representatives. The IWF Hotline is audited biennially by an independent team, led by a family court judge, and the report published in full.

Recommendations

2.1. That the Scottish Government works with the UK Government before seeking any amendments to Part 2 Schedule 6 of the Online Safety Bill to ensure that any amendments made are consistent with England, Wales, and Northern Ireland so that a consistent approach with how the four nations deal with CSE/A online can be maintained.

2.2. That the Scottish Government invests in preventative activity alongside the UK Government's Online Safety Bill, that seeks to address both demand for Child Sexual Abuse Images online and prevent them from being generated and appearing online in the first place.

2.3. Encourages the Scottish Government to continue and further extend its support for the IWF. By both supporting the potential role it could play as co-designated regulator for CSE/A in discussions with UK Government and by encouraging Education Scotland to become IWF Members.

Summary

3.1. The IWF has removed an increasing amount of Child Sexual Abuse Material from the internet over the last 25 years since we were founded. In 2021, we processed more reports than the entire first 15 years we were in existence and saw a **64%** increase in the amount of content we actioned compared with 2020.

3.2. The IWF is extremely concerned about the rise of self-generated Child Sexual Abuse Material, up **374%** in the last two years, and that this appears to be disproportionately affecting young girls.

3.3. Whilst the UK has a good track record on not hosting this content, it is concerning **that 550,000 to 8500,000** people pose a sexual threat to children in the UK.

3.4. The IWF has run several public awareness campaigns to raise awareness of these issues and we continue to play our part in the UK Safer Internet Centre and by running Safer Internet Day in the UK with the support of the Scottish Government every year.

3.5. Significant challenges remain, however, in how we improve online safety in Scotland and the UK. We welcome the UK Government's forthcoming Online Safety Bill and acknowledge that the Bill does give Scottish Ministers some freedom to introduce new definitions of CSE/A. As the UK hotline, we want to ensure that there is consistency in how we deal with CSE/A online because companies deploy our services not only in the UK, but globally, there is a need to ensure that these services are able to interact with not only UK but global standards too. The IWF does, however, remain open to improving the response to this threat online.

3.6. We remain concerned about the increasingly encrypted nature of the internet and in particular, the challenges End-to-End Encryption brings for child protection online and the complex international nature of this crime.
3.7. We believe the UK Government's forthcoming Online Safety Bill should build on best practice and strike a delicate balance in ensuring we do not push internet users into darker more complex online spaces to regulate.

3.8. We also believe that the Online Safety Bill will need other measures to complement it, including a much greater emphasis on prevention and ensuring that we prevent the generation of these images in the first place and prevent their circulation. This will also require us to address the issue of the large volumes of people who pose a sexual threat to children in the UK.

Scale and Nature of the CSE/A Threat

4.1. The IWF has just marked 25 years as a charity dealing with Child Sexual Abuse Material (CSAM) Online. Over that period, we have assessed **1.8 million** reports and actioned **970,000** reports for removal. Each of these reports can contain from one to thousands of individual images, meaning we have removed millions of child sexual abuse images and videos from the internet in the past 25 years.

4.2. In 2021, we investigated more reports of suspected child sexual abuse imagery than the entire first 15 years we were in existence. In the period 1996-2011 we assessed 335,558 reports and in 2021, we investigated **361,000** reports including from members of the public and our analysts own proactive searches. Of these reports, the IWF confirmed **252,000** reports as containing Child Sexual Abuse Material and the number of reports we actioned for removal in 2021, had increased by **64%** on 2020's figures. We have also witnessed over the past decade a worrying increase in the number of Girls appearing in these images. Ten years ago, Girls appeared in 67% of the imagery we removed, in 2021, it was **97%.**

4.3. Another concerning trend seen in our data over the last two years has been the rise in what we call "self-generated" indecent images of children. This is imagery that has been produced by children themselves via webcam and then uploaded, shared, or streamed online. Compared with our 2019 statistics we have witnessed a **374%** rise in this type of imagery, with the **11-13 age range of young girls** appearing most in this type of imagery.

4.4. In 2021, **147,900** reports contained self-generated indecent images of children, and this now equates for **59%** of all the reports we actioned. Concerningly, we also saw a three-fold increase amongst **7–10-year-olds** in the last year. In 2020, we saw 8,000 instances of self-generated child sexual abuse material in this age range and in 2021, this had increased to **27,000** a **235%** increase.

4.5. The National Crime Agency's recent Strategic Threat Assessment for 2021[2], estimates that as many as **550,000-850,000** people in the UK pose varying degrees of risk to children either online or offline. Their assessment also states that the Covid-19 pandemic and associated restrictions triggered temporary and permanent changes to the offending landscape.

4.6. Despite the concerning figures relating to the scale and nature of the threat, both in the generation of the imagery and the demand for the imagery online, the UK continues to have a robust response to this threat. In 1996, the year the IWF was founded, **18%** of the world's known Child Sexual Abuse Material was hosted in the UK. Today, that is less than **1%** and has been ever since 2003, thanks to the partnership approach that is taken between industry, civil society, Government and Law Enforcement.

4.7. **25 companies** in the UK were responsible for hosting Child Sexual Abuse Material in 2021 and **67 notice and takedown** requests relating to **350 webpages** were sent to these companies in 2021. Only 1 of these 25 companies was an IWF member.

4.8. The problem of where these images are hosted is largely an extraterritorial one. In 2021, we found **72%** of the content we actioned for removal was hosted in Europe (including Russia and Turkey) with the Netherlands responsible for **41%** of that content.

4.9. This imagery is often harvested from its original upload locations and then discovered by our analysts on image hosting boards and cyberlockers which account for **73%** and **10%** of the CSAM we removed from the internet respectively.

4.10. An image hosting board lets users upload images which are then available through a unique URL (webpage). These URLs can be made into online links, or be embedded into other websites, forums, and social networking sites.

4.11. A cyberlocker is a file hosting service, cloud storage service or online storage provider. They are internet hosting services designed specifically to host users' files.

4.12. It is important to recognise, that there is no one single entity that can give you a true understanding of the scale and nature of the CSE/A threat online. It would be impossible for us to estimate how many images are in circulation, but we believe that there are two conclusions we can draw from the figures we have outlined above about the scale and nature of CSE/A.

4.13. Firstly, over the past 25 years, the IWF, our industry partners and law enforcement have taken strides forward in the detection of this imagery. The creation of PhotoDNA in 2009 has enabled us to revolutionise our response to this issue and

[2] https://nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file

enabled us to create digital fingerprints (Hashes) of known child sexual abuse images that can be shared with companies to help them detect and prevent the upload of known material to their platforms. This is particularly important as victims of CSAM face the traumatic scenario of their images being reuploaded to the internet again and again. Hash technology can stop this. Our image hash list now contains more than **1 million unique hashes** which we share with our industry members. Our webpage blocking list (around 8,000-12,000URLS) deployed by our members, blocked at least **8.8 million** attempts from UK users to access known child sexual abuse material in the UK across three ISPs in one month in April 2020. We have all invested in more staff, technology, and tools to better detect this imagery and that can be one of the factors behind the rise in these numbers.

4.14. Secondly, however, and sadly, there is probably more content out there for us to find. Social Media has accelerated our use of digital technologies and its ubiquitous use amongst children and young people has undoubtedly enhanced and enriched their lives, but also bought with it significant challenges and risk of harm. Ofcom's Media Use and Attitudes report 2022, states that nearly all children (99%) went online in 2021 with the majority using a phone (72%) or tablet (69%) to do so. Their research also concluded 60% of children aged 8-11 had a social media profile, despite the minimum age being 13.

CSE/A definitions

5.1. Each individual report the IWF receives is assessed by one of our highly trained analysts. All our analysts complete a rigorous training and assessment process before they can assess any imagery and receive both in-house IWF training and, in addition, training from the National 5.2. Crime Agency to be certified assessors as part of the Child Abuse Image Database (CAID). Their assessment and judgments are trusted by law enforcement and the industry all over the world.

5.3. The key pieces of legislation used to govern our operations are listed on the IWF's website.[3] Perhaps the most important are the Protection of Children Act (1978) and the Sexual Offences Act (2003), that both apply in England and Wales and of relevance to this Committee is the Civic Government Act (1982) and the Protection of Children and Prevention of Sexual Offences Act (2005) as these apply in Scotland.

5.4. The Protection of Children Act (1978) and Civic Government Act (1982) creates the offence in law to take, make, distribute, or possess indecent images of children. The Sexual Offences Act (2003) and Protection of Children and Prevention of Sexual Offences Act (2005) sought to modernise the 1978 and 1982 legislation creating new legal offences, such as sexual communication with a child for example, but is also of importance to the IWF as linked to Section 46 of the Sexual Offences Act (2003) is our Memorandum of Understanding with law enforcement which permits our analysts to carry out their duties whilst being protected from prosecution and recognises our role

[3] https://www.iwf.org.uk/about-us/how-we-assess-and-remove-content/our-mou-the-law-and-assessing-content/

as the relevant authority for the reporting, assessment and removal of child sexual abuse imagery in the UK.

5.5. As we may also issue Notice and Takedown to companies who have hosting services based in Scotland, we have also sought clarity from the Crown Office and Prosecutor Fiscal Service that if we were to issue a notice to someone working in Scotland that they would not be prosecuted when acting in a professional capacity to remove CSAM. A letter[4] published on our website provides that clarity.

5.6. The IWF assesses Child Sexual Abuse Material according to the criteria and assessment levels set out in the Sentencing Council's: Sexual Offences Definitive Guideline (2014)[5]
5.7. The Indecent Photographs of children section (page 34) outlines the different categories of child sexual abuse material:

Category A: Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.

Category B: Images involving non-penetrative sexual activity.

Category C: Other indecent images not falling within categories A or B.

5.8. This categorisation of content is of vital importance as any images identified by our analysts as being confirmed as Child Sexual Abuse Material will be graded and added to the national policing database (CAID) and could therefore be used in criminal prosecutions against people caught in possession of these images.

5.9. Before the IWF can issue a Notice and Takedown for the content, we must check with the National Crime Agency CEOP referrals bureau that to remove the content wouldn't disrupt any ongoing police investigation. In most cases we receive permission to remove the imagery and that then enables the IWF to issue a notice and takedown request to the host of that imagery. The IWF has some of the fastest removal times anywhere in the world, thanks to our strong, collaborative relationship with UK industry, with our record for removing this content being **2 minutes** with **35%** of the content we actioned for removal in 2021, being removed **in under 2 hours** from the notice being issued.

5.10. The IWF is the only non- law enforcement agency with a connection to policing's Child Abuse Image Database (CAID). Any imagery we assess as illegal we add CAID and we are currently assessing 2 million Category A and B images from CAID to pass on to the internet industry, so that they can prevent the upload of these images and their distribution online.

[4] https://www.iwf.org.uk/media/5pmf45dp/legal-guidelines-for-hosting-companies-and-their-employees-in-scotland.pdf

[5] https://www.sentencingcouncil.org.uk/wp-content/uploads/Final_Sexual_Offences_Response_to_Consultation_web1.pdf

5.11. Under the proposals in the UK Government's forthcoming Online Safety Bill, Scottish Ministers will have the power (by way of regulations) amend Part 2 Schedule 6 of the Bill which relates to Child Sexual Exploitation and Abuse Offences. We would encourage Scottish Ministers to have conversations with UK Government before amending this schedule to ensure that there is consistency in the way that online child sexual abuse offences are regulated and dealt with under the law, particularly as this will have an impact on how IWF removes content hosted in Scotland.

Education, Awareness, and support

6.1. As stated earlier in this submission, one of the most concerning pieces of data from our recent statistics in the past two years has been the rise in "self-generated" indecent images of children appearing online. We have seen a **374% rise** in this content over the past two years and it mainly involves **11–13-year-old girls** and we have seen in 2021 an increase in younger children appearing in this imagery too**.**

6.2. In 2020, the IWF commissioned Zinc Network to work with us to create two public awareness campaigns to raise awareness and build resilience to the threat of self-generated Child Sexual Abuse Material online.

6.3. One campaign was aimed at parents and carers and was deliberately designed to shock parents about the scale and extent of child sexual abuse imagery online. The campaign's video used data from the National Crime Agency about the number of people in the UK that pose a sexual threat to children and encouraged parents to ensure they knew what their child was doing online in their homes and bedrooms, where parents thought they would be safe, to ensure that their home wasn't "an open front door to child sexual abusers." The campaign encouraged parents to TALK to their child about the issue of child sexual abuse online and how to stay safe online and had a dedicated website with a guide for parents and carers to provide information and support about how to have these conversations with your child.

T- Talk to your child about online Child Sexual Abuse

A- Agree ground rules about the way you use technology as a family

L- Learn about the platforms and apps your child loves and take an interest in their online lives

K- Know how to use tools, apps and settings that can help keep your child safe online.

More information about the T.A.L.K. campaign can be found on the campaign website[6] and the video designed to inform parents of the campaign can also be watched here. The parents campaign was distributed on Facebook, You Tube, Twitter and Google.

[6] https://talk.iwf.org.uk/

6.4. The second campaign was aimed at children and specifically 11-13-year-old-girls. The aim of this campaign was to raise awareness of grooming techniques used online, understand the different stats, facts and definitions of this issue and know what to do in the event of them receiving unwanted advances online.

The aims of the campaign were to get girls to:

- Think that inappropriate requests and messages for sexual content are not normal; they're abuse and a violation of their online spaces
- Feel outraged and motivated to keep their online space safe
- Not respond to inappropriate messages and requests, to block and report and tell someone they trust

6.5. The girls' campaign was distributed on Snapchat, Instagram, Tik Tok, Google and You Tube which consisted of graphics with key statistics, facts and definitions and included a manifesto film and influencer films. The Girls campaign video can be viewed here and the dedicated microsite is available to view here[7].

6.6. Surveys to assess the campaign's effectiveness were conducted one week before the launch of the campaign, one week after the initial six-week campaign phase and another after the conclusion of the campaign.

6.7. In the final evaluation of the campaign, we found that as many as **1 in 3 girls** had been affected by this issue, either directly or knowing someone that had received either a message requesting a nude or a message that had made them feel uncomfortable.

6.8. Amongst parents and carers, the term "self-generated online child sexual abuse" was low and once being shown a definition of the term, most agreed the issue was common, but only half saw their own daughter as being vulnerable.

6.9. Parents and carers ability to have a conversation with their child was linked to their knowledge. Parents who were more likely to have a conversation with their child knew about the terminology and had a better understanding of the tools they could use to restrict and monitor their child's activities online.

6.10. Daughters who had been spoken to by their parents about the dangers of the online world, were also better equipped to deal with inappropriate requests and take appropriate action such as talking to their parents or reporting the issue to the police.

6.11. The film targeting parents was view **8.8 million** times with the T.A.L.K. checklist being downloaded over **3,250** times and the website being visited over 108,000 times. **31%** of parents who had seen the campaign said that they had a conversation with their child about the issue over the next month compared with just 20% who had not seen the campaign video.

[7] https://gurlsoutloud.com/

6.12. The girls campaign received **17.6 million** impressions with the film being viewed in its entirety on **166,000** times and the dedicated microsite being visited on **26,000** occasions. Girls who had seen the film and campaign materials were more likely **(71%)** to ignore or block the request than girls who had not seen the film (66%).

6.13. Overall, 90% of girls suggested that they should tell someone if asked for a nude photo or video.

6.14. The IWF also makes up one third of the UK Safer Internet Centre alongside Childnet International and SWGfL and a responsible for co-ordinating Safer Internet Day in the UK each year.

6.15. In 2022, the theme for Safer Internet Day was All Fun and Games? Exploring respect and relationships online.

6.16. Research published on the day explored the relationships children have with online gaming. Of the children surveyed **71%** said that playing games made them feel happy and relaxed online and **66%** if children said that it had helped them to develop new skills such as determination and problem solving.

6.17. The research did, however, also highlight some of the downsides to life online. **78%** of children and young people had received friend requests from people they didn't know and **46%** had received requests or invitations to meet up with strangers in person. **73%** also stated that they had also seen someone being mean or nasty online.
6.18. **59%** of children surveyed also said they want to learn more about how to play games online safely.
6.19. In 2022, **54%** of children aged 8-17 had said that they had heard of Safer Internet Day and as a result 80% said they feel more confident about what to do if they are worried about something online with 72% saying that they had a conversation with someone about how to stay safe online.

6.20. **32%** of parents and carers had also heard of the day with **67%** talking to their child about how to use the internet safely and **69%** saying they had a better understanding of how to keep their child safe online.

6.21. A record **3,424** organisations, schools, governments, police forces, charities and wider supporters signed up to support Safer Internet Day in 2022, with **936,666** views of the Safer Internet Day film and over **125,000** downloads of the education packs for use on the day.

6.22. 41% of teachers said the day also had led to an increase in safeguarding disclosures being made. The UK Safer Internet Centre is also grateful to the support it received from the Scottish Government who also participate in running workshops to help determine the theme for Safer Internet Day and this year also launched a new Parents Club Scotland Campaign to provide useful hints and tips for parents to help keep children safe online.

Challenges

7.1. **European hosting of content-** As mentioned previously in this evidence, Europe is the global hotspot for the hosting of Child Sexual Abuse Material. **72%** of CSAM we removed from the internet in the last year was hosted in Europe and this is mainly hosted on image hosting boards and cyberlockers. We are looking forward to seeing the detail contained within proposals soon to be published by the European Commission on how to tackle child sexual abuse material in Europe, but the European Commission's impact assessment for their forthcoming proposal also points to wider challenges with the implementation of the current directive by Member States, with the European Commission having opened infringement proceedings against 23 of the 27 for possible non-conformities.

7.2. Whilst this might not appear directly relevant to the UK situation or Scotland, the challenge is that this is a global problem. Just because Scotland and the UK has a good record on not hosting this content, does not mean that children in the Scotland and the UK cannot come to harm. A child in Scotland could be groomed by an offender in another country into creating self-generated material that may be hosted on a server located in the European Union. Only by working collaboratively and addressing these hosting issues will we be able to prevent harm occurring to children.

7.3. **Increasing moves toward greater encryption online-** For the last five years, the IWF has been warning about the dangers of the internet moving towards greater encryption online without considering the need for child safety online.

7.4. It is important to say from the outset that the IWF is not against strong encryption. Encryption is not simply a good thing to be pursued at all costs or a bad thing to be avoided. Improvements in encryption have, for the most part, been a good thing. Standard encryption has revolutionised the way we browse the web, access banking and government services, and how we communicate via email and messaging apps.

7.5. Until recently, privacy and security developments have largely been compatible and complementary with the systems that have been protecting the safety of our most vulnerable web users. This includes systems used by social media, messaging, and data storage platforms to automatically detect images and videos of child sexual abuse material.

7.6. Deploying End to End Encryption (E2EE) in communication and social media platforms, is however, different. E2EE extends standard encryption so that only the sender and receiver can view the content of the messages. This prevents the platform themselves from accessing any data being hosted on or passed through their systems. It is important to remember that all popular messaging platforms are already using standard encryption which prevents our data from being intercepted by third parties.

7.7. Whilst encrypting messages so the tech provider can't see the content might appear to be a good thing, "turning off the lights" as the National Crime Agency puts it, also means technology platforms lose the ability for lawful access, and crucially, will not be able to automatically detect images and videos of child sexual abuse being hosted or shared through their systems.

7.8. We have seen that social media companies are doing some amazing work to detect known child sexual abuse images. In 2020, Meta reported 20.3 million reports of known CSAM to the National Center for Missing and Exploited Children (NCMEC) in the United States using mainly hashing technology to detect these reports. But we have also seen the impact of what happens when they do not scan for content, when changes to EU privacy rules in the first half of 2021, saw them switch off voluntary scanning leading to a 58% reduction in reports from EU accounts.

7.9. We must ensure that the pursuit of individual privacy online is not at the expense of victims of child sexual abuse or their right to privacy and their right not to have their images and videos of their abuse freely circulating online. We must ensure that efforts to protect privacy do not compromise child safety.

7.10. The problem of online child sexual abuse and exploitation is a growing problem, and we must be careful to ensure we do not take steps backwards, giving up some of the best technological solutions we have in the fight against it.

7.11. The IWF would urge technology companies to take a balanced approach to user privacy and child safety. We would like to see industry leaders taking other steps to improve user privacy before adopting E2EE or at least develop effective tools for detecting CSE/A content and child safety tools that are compatible with E2EE environments.

7.12. We would like to see tech companies focussing on how we resolve current challenges such as the rise in self-generated content before and the identification of new content and moves towards E2EE will simply make responding to these challenges even harder in the future.

7.13. We believe that the joint committee appointed to scrutinise the Government's draft Online Safety Bill made a sensible recommendation to include E2EE as a specific risk factor in risk assessments and profiles and that service providers should be required to mitigate risk arising from the encrypted nature of their services under the safety by design requirements.

7.14. **Virtual Private Networks (VPNs)-** Linked to E2EE, the IWF is also concerned about the increasing prevalence, availability and easy access to VPNs which can often be used to circumvent parental controls and other content filtering solutions provided by ISPs. We need to ensure that content blocking mechanisms, such as those proposed through Clause 124 in the Online Safety Bill do not see unintended consequences such as individuals downloading VPNs and ending up in more extreme parts of the internet and on the dark web. We would recommend that Government ensure VPNs are also putting in place protections to ensure they are not allowing customers access to CSAM.

7.15. **Online Safety Bill and co-designation-** The UK Government will shortly be introducing its Online Safety Bill aimed at making the UK the safest place in the world to go online and in ensuring the strongest possible protections are in place for children.
7.16. The IWF is supportive of the UK Government's ambitions to improve online safety and we have been actively engaged with Government on the development of the legislation and been in consultation with the Scottish Government around some of the responsibilities contained within the Bill which are devolved matters and where we believe the Bill can be strengthened further.

7.17. We believe that the Bill should build upon current best practice, consider the technical expertise that will be required to effectively regulate this space, and ensure it respects current international collaboration that already exists in this space.

7.18. The IWF wants to ensure that its skills and expertise is reflected in the forthcoming regulatory environment, and we believe this is best achieved through co-designation to regulate CSE/A with Ofcom. The Government's Online Harms White Paper, the Government stated:

"It would work with Ofcom to ensure that the regulator is able to work effectively with a range of organisations. This includes through a range of means including co-designation powers, memorandums of understanding, forums, and networks."

7.19. However, the current draft of the Online Safety Bill does not explicitly mention either co-regulation or co-designation or how the Government and Ofcom intends to achieve this. The Draft Online Safety Bill committee recommended that Ofcom should be given the power to co-designate efficiently and effectively and stated that the IWF had

"Made a persuasive case that they should be co-designated by Ofcom to regulate CSE/A content an argument which had been supported by both the Crown Prosecution Service and Talk-Talk."

7.20. The IWF is continuing its discussions with Ofcom, Government, and the National Crime Agency about how we continue to work with these partners in the future, but believe more clarity is needed ahead of the Bill becoming operational on how all these functions will work together and work collaboratively. We support the suggestion made by the draft Online Safety Bill committee that more information is required on how co-designation may be achieved.

7.21. **Mandatory Reporting-** The IWF is also supportive of the introduction of mandatory reporting in the forthcoming Online Safety Bill. This requirement will be placed on all companies in scope of the Bill as well as Internet Service Providers (ISPs) and other infrastructure providers not covered in the Bill's definition as either providing User-to-User or search services.

7.22. The mandatory reporting element will require companies who are not currently reporting elsewhere to report any CSE/A content with links to the UK to the National Crime Agency as the designated body.

7.23. The IWF believes the benefits of introducing mandatory reporting will include an ability to better understand the scale and nature of the threat along with transparency reports from companies which are also required within the Online Safety Bill. The IWF is, however, keen to ensure that the reporting structure complements existing international structures, such as US companies reporting to the National Center for Missing and Exploited Children (NCMEC) in the United States and plans in Europe for a new Centre to tackle Child Sexual Abuse and its own introduction of mandatory reporting in plans to be announced by the European Commission on 11 May 2022.

7.24. **Membership of IWF-** In November 2021, the IWF welcomed the Welsh Government's Digital Learning Division as a Member, becoming the first Government to join the IWF through membership. The IWF is currently in discussions with Education Scotland, and we look forward to hopefully welcoming them as Members soon.

Scottish Biometrics Commissioner

3 May 2022

Dear Convenor,

Criminal Justice Committee Roundtable Evidence Session on 18 May 2022: Tackling online Child Abuse, grooming and Exploitation

I refer to the call for evidence to support the above discussions and would offer the following brief comments relative to where such issues intersect with my functions as Scottish Biometrics Commissioner.

Firstly, and as the Committee will be aware, the true nature, extent, and impact of online child abuse, grooming, and exploitation is difficult to ascertain. There are however three things of which we can be certain. The first is that all available evidence suggests that such offending is on an upwards trajectory. The second is that whilst online child sexual abuse takes many forms, all are unquestionably child abuse. The third is that the scale of the challenge cannot be met by law enforcement alone.

In February 2020, HMICS published a strategic review of Police Scotland's response to online child sexual abuse.[8] This was followed up in August 2021 with a progress review against the ten recommendations previously made.[9] These reports by HMICS more than adequately capture areas where there is room for improvement in the policing of such matters.

In relation to the investigation of such offences, Police Scotland will regularly acquire, retain, use, and destroy materials constituting biometric data within the definition of section 34 of the Scottish Biometrics Commissioner Act 2020, primarily images and recordings. As highlighted by HMICS in 2020, there are over fourteen million images in the UK Child Abuse Image Database (CAID) alone and over 250,000 videos. Police Scotland is a user of, and contributor to that database.

Where Police Scotland use such data as part of overt policing activity then such data would fall within the oversight of the Scottish Biometrics Commissioner. However, my remit does not extend to biometric data obtained through covert policing activity under the Regulation of Investigatory Powers (Scotland) Act 2020, as these are reserved

[8] HMICS Strategic review of Police Scotland's response to online child sexual abuse, February 2020: https://www.hmics.scot/sites/default/files/publications/HMICS20200226PUB.pdf

[9] HMCS Progress review of Police Scotland's response to online child sexual abuse, August 2021: https://www.hmics.scot/sites/default/files/publications/HMICS%20Progress%20Review%20of%20Police%20Sc
otland%27s%20response%20to%20online%20child%20sexual%20abuse%20and%20exploitation.pdf

matters within the authority of the UK Investigatory Powers Commissioner (IPCO). I also have no authority over biometric data collected by UK-wide bodies operating in Scotland.

One area of concern that is widely acknowledged around such investigations whether overt or covert is that of demand outstripping capacity in relation to evidential recovery through digital forensics techniques. Another is the absence of accreditation of the techniques deployed in Scotland in relation to digital forensics laboratory work.

Both HMICS and the SPA have previously recommended that Police Scotland should pursue accreditation of its digital forensics' laboratory work. In 2020, the SPA Digital Forensics Working Group recommended that Police Scotland should adopt the ISO 17025 quality standard by 2022. Police Scotland subsequently agreed to pursue this in May 2021, but I understand that it is likely to be 2024 before compliance is achieved.

My concern is that where digital material constituting 'biometric data' (primarily face and voice) is recovered in circumstances where it has the potential to enter the evidential chain from crime scene to court then it is essential that the scientific validity and reliability of the underpinning techniques deployed are beyond reproach. This is necessary to ensure that exculpatory evidence essential to the defence is not inadvertently overlooked.

To illustrate the complexity of such cases, I would draw the Committee's attention to the two case studies relative to online child abuse contained within page 15 of the SPA Digital Forensic Working Group report: https://www.spa.police.uk/media/flediwqv/rep-b- 20200424-item-8-digital-forensics-wg-report.pdf as these illustrate the often industrial scale of offending in such cases.

As intimated at the outset, the nature and extent of this problem is such that it cannot be met by law enforcement alone. For me there are three key prevention areas which would deliver the greatest return on investment beyond policing. Those are:

1. Online safety education and training for children, young people and parents or guardians.
2. Technical solutions such as parental controls.
3. A duty of care and legal responsibility for website hosts and social media platforms who clearly have the technical capacity and capability to do more

I trust that these brief comments are of assistance.

Yours sincerely

Dr Brian Plastow
Scottish Biometrics Commissioner