LUCY FAITHFULL FOUNDATION

Input to the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children

Background

The Lucy Faithfull Foundation is a UK wide child protection charity that is unwavering in its commitment to preventing child sexual abuse and exploitation. We are in a unique position because we are one of only a few organisations tackling the problem at source by working with those perpetrating abuse or at risk of doing so. We run the Stop It Now helpline, the largest helpline of its kind in the world for people concerned about their own sexual thoughts and behaviour towards children and anyone concerned about child sexual abuse, and we support more than 8,000 callers who make more than 16,700 calls each year. The reach of our online self-help is even wider with over 400,000 users accessing it last year. Annually, we asses risk in hundreds of adults and adolescents and provide groupwork interventions to several hundred more. Where abuse has occurred, our teams advise statutory agencies on case management and provide intervention programmes to rebuild family safety. Our preventative work includes early intervention programmes for families considered at risk of harm and public education. We also work to prevent harmful sexual behaviour amongst young people through our work in schools and our programmes designed for young people themselves. This includes our website and live chat service Shore. The only resource of its kind in Europe and one of only three in the world, Shore is for young people concerned about their own sexual thoughts or behaviour or that of a friend. In addition, we deliver training across the UK and the sector, reaching more than 2,000 frontline workers a year, including those in law enforcement, education and social care.

Our mission is simple – to prevent child sexual abuse and exploitation. It is this mission that draws all of our varied services together because child sexual abuse is preventable, not inevitable. It is with this mission in mind and over 30 years of experience in working to prevent child sexual abuse that we have approached this call for inputs by the Special Rapporteur for this thematic report.

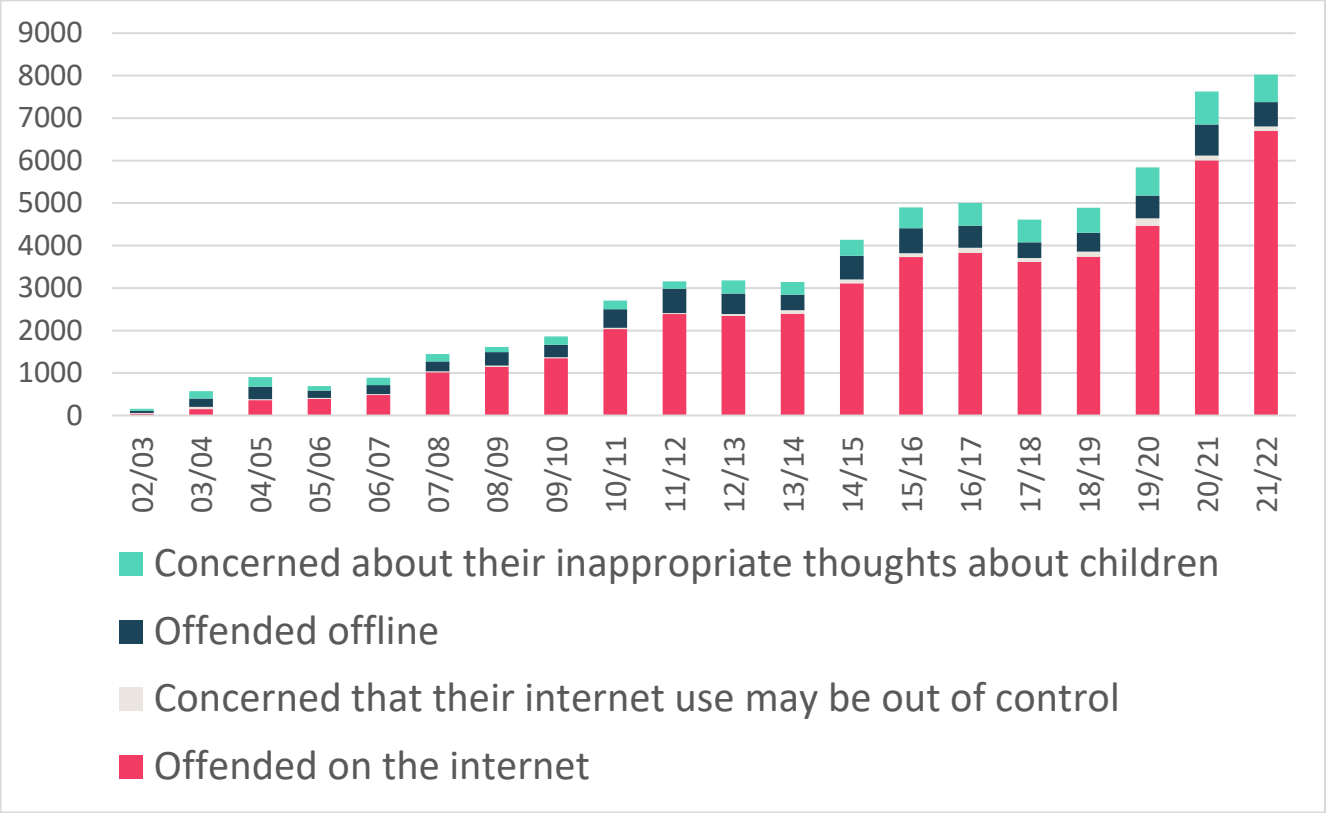
We have considered the 9 guiding questions for submissions and we have prepared our input around the following four themes:

1. Impact of technology on child sexual abuse;
2. Recommendations for the prevention of online child sexual abuse;
3. Setting a global example through regulation in the UK; and
4. Challenges posed by AI

Impact of technology on child sexual abuse

We have been running the Stop It Now helpline since 2002 and the graph below shows the significant impact that technology has had on calls to our helpline over the past twenty years. Calls to our helpline have increased year on year, but this has been overwhelmingly driven by the increase in child sexual abuse offending online. The majority of our calls come from adults concerned about their own behaviour and the increase in calls about online offending within this target group is clearly evidenced below.

Calls to the Stop It Now helpline from adults concerned about their own behaviour



In response to the increase in online offending, we have developed a number of projects and services including:

- Inform Plus and Engage Plus – programmes in which we work with individuals to stop online offending. Inform Plus has been running since 2005 and helps individuals to stop viewing indecent images of children whilst Engage Plus has been running since 2019 and is directed at stopping online sexual communications with children.
- Online deterrence campaign – a multi-channel communications campaign which includes press, PR, and digital advertising aimed at raising awareness of online child sexual abuse and specifically targets those concerned about their own online behaviour to seek support from our Stop It Now services.
- Project Intercept – a £1million initiative which is seeking to revolutionise how we stop online child sexual abuse by using behavioural science, partnerships and innovation to rollout effective online warnings across the internet.

In addition to increased contact to our Stop It Now helpline in relation to online offending, we also believe that technology has contributed to a rise in peer on peer sexual abuse and harmful sexual behaviour amongst children and young people. We have responded by developing services that aim to prevent harmful sexual behaviour including:

- Inform Young People – an educational programme for young people in trouble with the police, their school or college for inappropriate use of technology and the internet which we have been running since 2012.
- Everyone's Safer – a three year action-research project to develop effective leadership responses to harmful sexual behaviour in schools, working with 10 secondary schools each year.
- Shore – a website for teenagers which provides a safe space for them to learn about sexual relationships and behaviour that was launched in 2023. In addition to clear and reliable information provided by the website, confidential and anonymous support is available for young people through Shore's chat and email service.

Whilst we work to prevent child sexual abuse both online and offline, there is no doubt that the use of technology has over the past two decades had a significant impact on the scale of offending and the services and projects we have developed in response.

Recommendations for the prevention of online child sexual abuse

In 2020, the National Crime Agency in the UK reported that investigators were able to access illegal child sexual abuse material in just 3 clicks on the open web. We believe that four years later, that may have increased to 4 clicks. But we need to get to a place with online regulation where such material cannot be accessed no matter how many clicks.

The fact remains that law enforcement is not currently able to keep up with the sheer volume of offending which is happening online. It has long been the mantra within law enforcement that "we cannot arrest our way out of the problem" and therefore a whole system approach is needed to deal with a problem of such significant scale and nature.

The Centre of expertise on child sexual abuse estimates that 500,000 children are sexually abused every year in the UK. The National Crime Agency estimates that up to 850,000 individuals pose a sexual risk to children in the UK. And law enforcement in the UK is currently recording 105,000 child sexual abuse offences per annum. These figures, although not specific to just online offending, are indicative of the gap between the volume of offending and the proportion which is being met with a response from the criminal justice system. We believe that these statistics which are specific to the UK are also reflected in other countries around the world.

Given the gap between what the criminal justice system is able to address and the scale of online offending, we believe that there is need for:

1. Services equivalent to our Stop It Now helpline;
2. Online deterrence campaigning;
3. Online warnings; and
4. Additional frictions that confront online offending behaviour.

Services equivalent to our Stop It Now helpline

As described above, law enforcement is not currently able to keep up with the sheer volume of offending which is happening online in the UK, therefore a whole system approach is needed to deal with a problem of such significant scale and nature. The same can be said for all countries around the world.

This leaves an important role for our Stop It Now services. In the instances where individuals have been arrested, it is common practice amongst many police forces across the UK to refer arrested individuals to our Stop It Now helpline. We work in conjunction with the criminal justice system in cases where individuals have been arrested to take steps to prevent future offending.

But there are additional roles for our Stop It Now services. For individuals who have offended online but are not known to the authorities, we offer confidential and anonymous support so that they can stop their offending behaviour and stay stopped. Further, for individuals who have not yet offended but may be at risk of doing so, we also offer confidential and anonymous support to help them take the necessary steps to ensure that offending does not happen. We intervene early to prevent the escalation of problematic behaviour before an offence takes place and a child is harmed.

There are a number of equivalent services in a handful of countries such as Stop It Now in the USA, Australia, the Netherlands and Belgium, as well as Talking for Change in Canada, and the Dunklefeld Project in Germany. However, it remains the case that the majority of countries around the world do not have equivalent services. We therefore recommend that services like Stop It Now become available on a global scale. Given our history of supporting the development of projects, including Stop It Now Netherlands and Australia, we would be delighted to talk about this further.

Online deterrence campaigning

Since 2015, we have, each year, been running our online deterrence campaign which seeks to deter people from online child sexual abuse offending, in relation to both indecent images offences and grooming offences, with the latter added in 2019. Our online deterrence campaign is a wide-reaching multi-channel communications campaign which includes press, PR, digital advertising and regional partnerships with relevant agencies, such as law enforcement and the National Health Service.

Through research conducted with arrested individuals in our pilot evaluation, we identified that key messages to get across in any campaign seeking to deter people from online child sexual abuse offending include:

- It's a crime;
- It causes harm;
- It has serious consequences;
- There is help to stop.

Each year, our deterrence campaign is independently evaluated and the learnings and insights drawn are fed back into the development of the next phase of the campaign and this continues to be the case. Over the years, these evaluations have shown that the campaign brings offenders who have not yet been arrested to our services and they report positive changes in attitude and behaviour including stopping risky and illegal behaviour after seeking our support. Further details regarding our online deterrence campaign can be found in our Faithfull Paper (2023) *Deterring online child sexual abuse and exploitation: lessons from seven years of campaigning*.

We have learned from our online deterrence campaigning over the past decade that some people that need help will seek it if they know that it is available and confidential. In addition, deterrence messaging and effective support can mean that people do not offend in the first place. For those that have already offended online, self-reported behaviour change is possible.

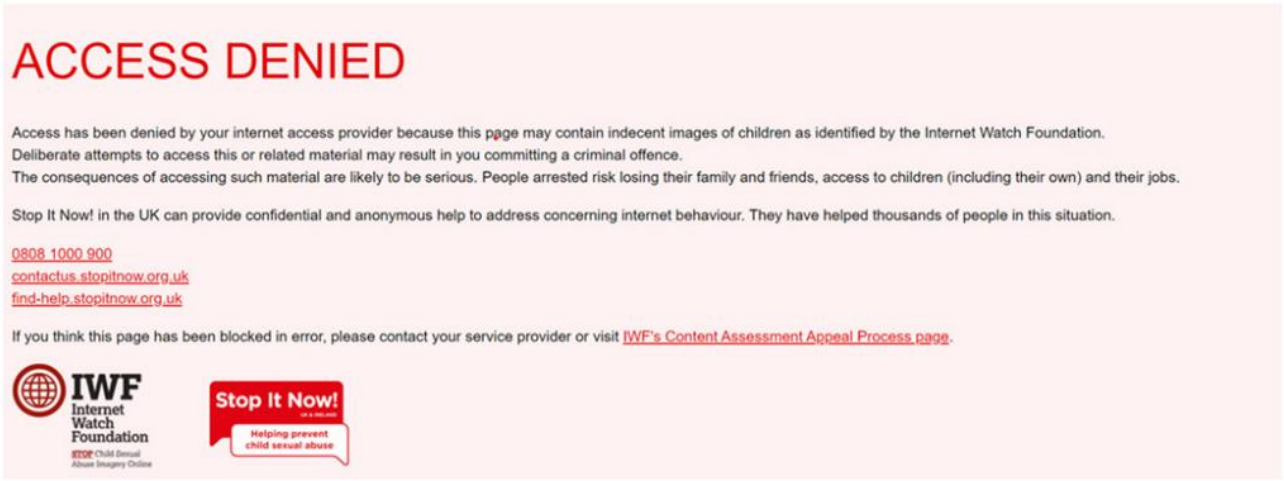
Our online deterrence campaigns have been successful and so, similar to our recommendation for services equivalent to our Stop It Now on a global scale, we also recommend that online deterrence campaigns should be utilised on a global scale.

Online warnings

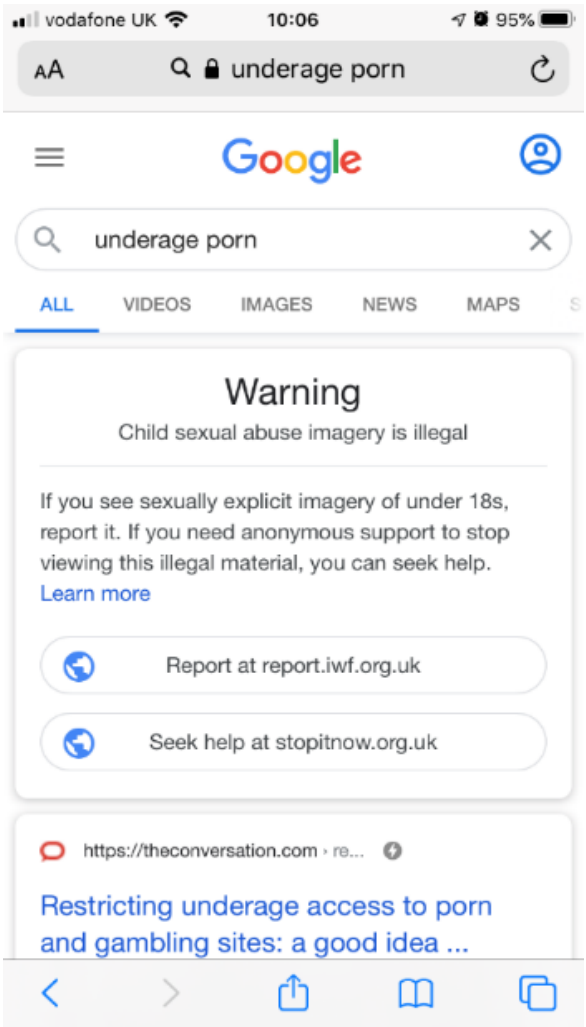
For almost a decade, we have been working with tech companies to pioneer the use of online warnings to deter online child sexual abuse offending, replacing the previous error 404 messages. Through splash pages (for blocked URLs) working with the Internet Watch Foundation (IWF) and in collaboration with tech companies like Google, Meta and Aylo, we developed online warning messages to be deployed when people attempt to search for child sexual abuse material or visit URLs that are known to host it. These deterrence messages warn the user of the illegality of what they are attempting to do and signposts to our Stop It Now services for help to change their behaviour.

Examples of current online warnings are shown below:

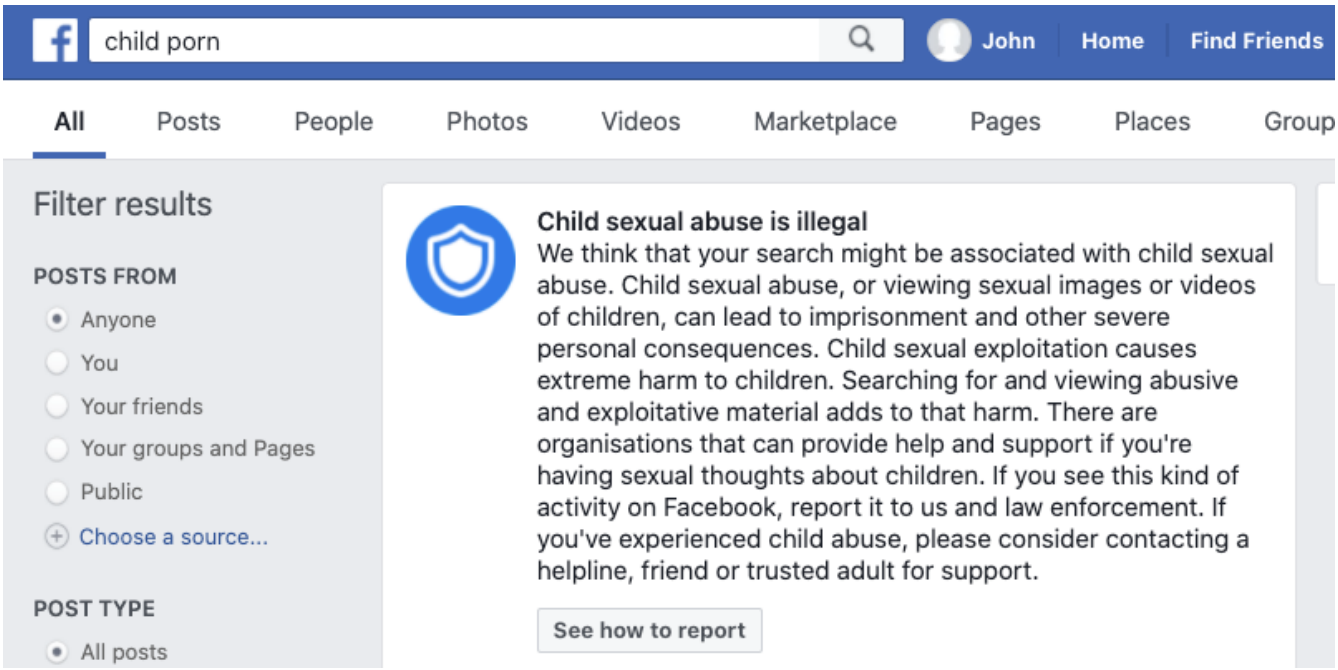
IWF splash page



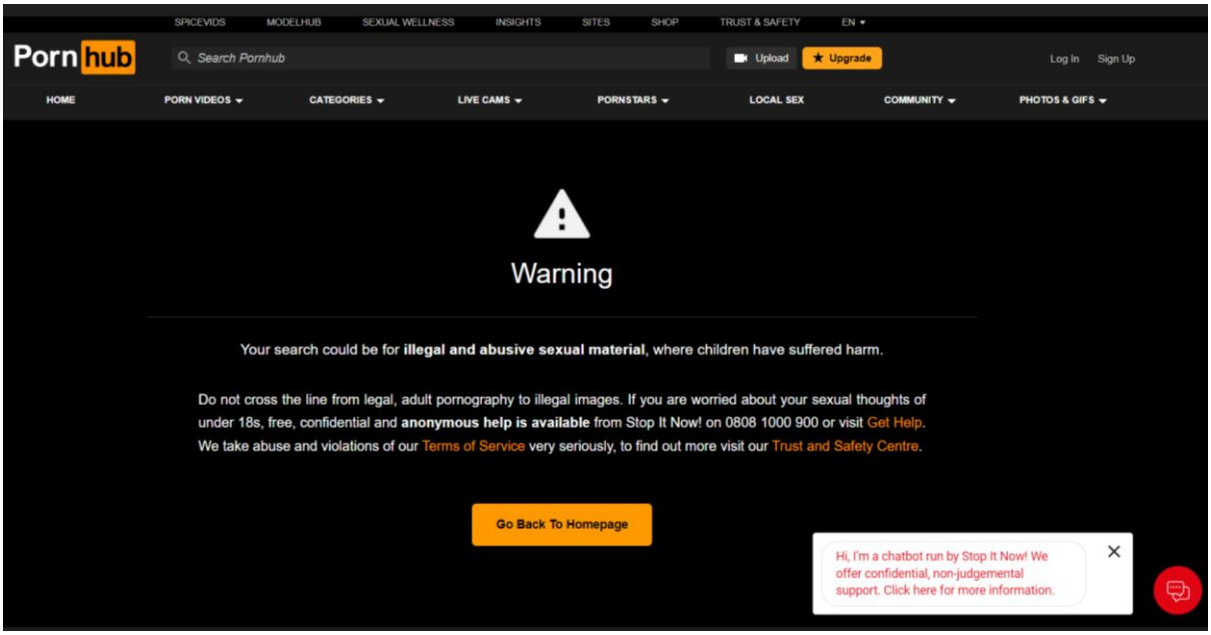
Google warning in the UK



Facebook warning



Evidence that supports the use of online warnings can be found in the recently published evaluation of the reThink Chabot project, a collaboration we undertook with the IWF and Aylo to deploy a chatbot on Pornhub UK which is triggered when a user makes a search associated with seeking illegal underage content. The appearance of the chatbot currently is this:



The independent evaluation was carried out by the University of Tasmania, and key findings from the report include:

- 99.8% of sessions during the evaluation period (March 2022 to September 2023) did not contain a search that triggered a warning;
- The chatbot was displayed 2.8 million times during the evaluation period;
- This resulted in 1,656 requests for more information about Stop It Now services;

- There were 490 click-throughs to the Stop It Now website and approximately 68 calls and chats to the Stop It Now helpline;
- There was a statistically significant trend showing a decrease in the number of searches for CSAM on Pornhub UK during the evaluation period;
- The warning message and chatbot reduced the total number of searches for CSAM;
- Most sessions which triggered the warning and chatbot once do not appear to have searched for CSAM again; and
- Those who saw the warning message more than once tended to undertake non-CSAM searches after receiving the warning.

The chatbot is a first of its kind in the world and the evaluation is hugely important in showing the effectiveness of this type of deterrence intervention in both reducing searching for child sexual abuse material on the platform and directing individuals to Stop It Now services.

This evaluation is important evidence that shows that warning messages, however delivered, whether it is a static warning page or via a chatbot, are effective. Consequently, we recommend that online warnings be scaled across all platforms in all online spaces so that warnings become the norm rather than the exception. As referenced above, we are currently working to do this in our Project Intercept. We believe that it is a simple additional step after detecting, blocking, removing and reporting online child sexual abuse, to engage the user whose behaviour is problematic and direct them to support to change their behaviour. For too long we have relied on influencing the behaviour of children, we need to place greater emphasis on influencing the behaviour of those who seek to cause harm.

Additional frictions that confront online offending behaviour

In addition to online warnings when a user is seeking child sexual abuse material, we believe that additional frictions can be created to confront other online offending behaviour such as grooming. One area that is often considered by tech companies to combat this harm is the use of default settings for child user accounts. Whilst we think that it is important to have such safeguards in place, we also think that this should be combined with creating friction on the other side as well, that of the perpetrator or potential perpetrator. The responsibility ought to be not on children to protect themselves but on those seeking to harm children not to offend.

One example of this relates to tactics adopted by perpetrators to groom children online which include: sending scattergun friend requests to large volumes of children; infiltrating the online friendship groups of children that perpetrators have succeeded in connecting with; and sending unsolicited direct messages to children that are not connections.

Taking first of all the scattergun friend requests to a large number of children, we question why frictions do not exist when such a request is made to a large number of children? Is that perpetrator prompted with a warning? If not, why not? It is certainly common in many workplaces for communications such as emails to a large number of people to be stopped and the sender to be prompted with a question regarding their intention. This is usually done for data protection purposes and could similarly be applied at this stage of the grooming process.

And, when a perpetrator is trying to communicate with a child for the first time, is the perpetrator prompted with a warning? If not, why not? Again, it is common in other areas of life for prompts to be in place when making contact for the first time. An example can be taken from online banking. It is common in making a payment to someone new to be prompted by questions like whether the user knows the person and warnings about fraud. Of course, not all payments to someone new are fraud, and likewise not all new communications with a child are attempts to groom but this sort of intervention could be similarly applied to create friction in the grooming process.

We believe an evidence-base likely does exist in relation to other harms where such practices are commonplace such as detecting fraud and preventing data breaches. We also believe that these practices commonly used to combat fraud and prevent data breaches could be adapted and applied in contexts to prevent child sexual abuse and exploitation and done so on a global scale.

Setting a global example through regulation in the UK

After many years in the making, the UK's Online Safety Act received royal assent in October 2023 and marked a watershed moment. The Online Safety Act has ushered in a new regime for regulation of the technology industry in the UK, establishing Ofcom as the regulator.

Looking ahead, tech companies will be required to meet certain standards set down by Ofcom. There is still much work to do in order to implement the Act and Ofcom is currently consulting on the first code of practice for illegal harms which includes child sexual abuse and exploitation. It will take time before Ofcom's powers start to bite, the bar set by the standards will be increased incrementally and it will take a series of steps rather than one giant leap to get there. But, the technology industry will no longer be permitted to regulate themselves, a path that clearly has not worked and the sanctions imposed could be substantial with potential fines or imprisonment for tech bosses and large-scale fines on the companies themselves for non-compliance.

The UK has set an important example in adopting the Online Safety Act and we are hopeful that more countries will follow suit with legislation being debated in other countries, such as the EU and Canada. The need for online regulation in more countries is clear as online child sexual abuse and exploitation knows no borders and that regulation needs to be aligned. It is good to see the establishment of the Global Online Safety Regulators Network and we very much hope that this network of online regulators will grow in the years to come.

Coalitions have played an important part in the road leading to online regulation in the UK. The children's sector came together during the passage of the Online Safety Bill through Parliament to speak with a louder joint voice, and support the advocacy efforts of each other and specific amendments to the Bill. Coalitions continue to play their part in the work ahead, for example the Online Safety Act Network which brings together civil society organisations, researchers and campaigners, all with the common shared goal of successful implementation of the Online Safety Act. We believe that coalitions in other countries can learn from the experiences of the children's sector in the UK as they help to shape regulation in their respective jurisdictions.

Challenges posed by AI

Like other child protection organisations around the world, the impact of AI generated technology has started to affect our work. AI is no longer an emerging threat but instead is one that we are grappling with in the here and now. In this part of our input, we will address:

1. The impact of AI on calls to our Stop It Now helpline;
2. An AI case study from our work in schools; and
3. Our views on some of the global challenges presented by AI technology.

The impact of AI on calls to our Stop It Now helpline

Most notably, we have started to see calls to our Stop It Now helpline in relation to AI-generated child sexual abuse material. These calls began in the latter part of 2023 and over a 5 month period from November 2023 to April 2024, we recorded 36 calls to our Stop It Now helpline involving generative AI.

The number of AI-related calls are a very small proportion of the total calls we handle each year. In 2022/2023 we took 16,764 calls, emails and chats via our Stop It Now helpline, thus 36 AI-related calls over a 5 month period represents a small fraction. However, we expect the number of AI generated calls to grow significantly over the next few years. We are therefore upskilling our staff, particularly our Stop It Now helpline advisers to be able to identify and ask questions about generative AI, and to respond and record it accordingly.

We are already seeing a breadth in terms of the AI-related calls we have received and these calls are affecting all of our caller groups. The majority of the AI-related calls were from individuals concerned about themselves and their own behaviour, this is true also of calls to our Stop It Now helpline which

do not concern generative AI. But we have also received calls from adults concerned about another adult, adults concerned about a young person and professionals seeking help.

The table below gives a snapshot of a few of the AI-related calls we have had across our different caller groups:

Arrested individual
Isaac, 56, contacted the helpline in January 2024 having recently been arrested for possessing AI generated sexual images of children that he had sourced from Twitter/X. He said that he had been struggling with a long-term pornography addiction, which was exacerbated by stress, mostly related to work. On further exploration, it became apparent that Isaac had a long-standing sexual interest in children, too, and that he felt exploring AI images was less harmful than seeking out images of real children.
Partner
Josie, 25, had found the helpline details on Google. She contacted us after her long-term partner, Steven, disclosed that he had been accessing animated sexual drawings of children online. Josie was worried about the significance of this content and potential consequences for Steven.
Parent
Jacklyn, 35, contacted the helpline with concerns about her 13-year-old stepson, Marcus. Jacklyn had found an image on Marcus' mobile phone of her face merged, using an AI app, with a naked body. She reported feeling shocked as she had never had any prior concerns about his behaviour. She had not yet spoken with Marcus or her husband about this matter and was not sure how to broach the subject or whether it was best to say nothing.

An AI case study from our work in schools

We are also starting to see the impact of generative AI through our work in schools in the UK. Our Everyone's Safer project is an action research project that supports schools and education staff to prevent and respond to harmful sexual behaviour. Across 3 years, we are working with 10 schools each year and generative AI has featured in this work, exemplified by the following case study:

- Three female students, aged 12 and 13, reported to the safeguarding lead at their school that other students told them they had seen nude images of the girls.
- School staff investigated and students reported a male student aged 13 had shown the nude images.
- Police were contacted and student mobiles were confiscated.
- Police investigation revealed the male student downloaded a freely available 'nudify' app to create the images.
- Many of the students believed the girls had posed for the images and so were judged and shamed by their peers.
- The girls reported feeling violated and humiliated.
- Police investigation is ongoing and the male student could face criminal charges.

The impact from this harm is far-reaching: from the three girls who suffered harm and the families supporting them to the young boy who used AI technology to cause the harm, and the uncertainty facing him and his family, but also all the children in the school who viewed the AI generated images and those that did not but were aware of it, to the teachers, staff and wider school community.

Our views on some of the global challenges presented by AI technology

Here in the UK, it is illegal to create, view or share sexual images of under-18s, including images that have been created using AI technology. But this is not universally the case around the world. It is imperative that countries that do not have equivalent legislation that ensures AI generated sexual images of children are illegal, take immediate steps to close the gaps.

AI generated material is hugely harmful. Often AI technology is being used to manipulate images of real children, some of whom have previously been victims of sexual abuse. Real children find themselves being victimised again and again as offenders create new sexual imagery using AI technology and distribute the imagery online.

AI generated sexual images of children, however they are created, normalises the sexualisation of children and is dangerous.

Even when AI generated imagery is illegal as it is here in the UK, there is still work to be done to inform the public of this and warn of the danger. We carried out a recent public survey which found that 40% of those surveyed in the UK did not know or thought that such imagery was legal in the UK despite the law being clear that it is illegal. Further details of this research can be found in our blog.

Given the lack of clarity amongst the public, there is a real opportunity for collaboration with tech companies for deterrence messaging of the sort that we have discussed earlier in this response. Online warnings are not only able to inform those seeking to use AI technologies to cause sexual harm to children that it is illegal but can engage the user whose behaviour is problematic, divert them from their course of action and redirect them to support to change their behaviour from services like Stop It Now. AI models need to be stopped from producing this material but at the same time, users seeking to misuse AI technology with prompts to create such material should also be confronted with a warning. Our recommendations to prevent online child sexual abuse set out above in our view can equally be applied to the specific challenges posed by AI technologies. We also believe that many existing global structures that are already working to tackle online child sexual abuse and exploitation such as the WeProtect Global Alliance, the Tech Coalition and the Virtual Global Taskforce are also well suited to direct their energies to responding to the threats posed by AI.

We would be happy to discuss any aspect of this submission in more detail.

Frances Frost **|** Director of Policy and Advocacy
ffrost@lucyfaithfull.org.uk **|** 07749 492432
lucyfaithfull.org.uk

31 May 2024