

Briefing from the Internet Watch Foundation: Criminal Justice Bill Report Stage

Key asks:

1. That MPs speak in favour of **New Clause 25**- “The offence of possession of a guidance on creating child sexual abuse material”.
2. That MPs speak in favour of **New Clause 26**- “The offence of simulating sexual communication with a child”.
3. That MP’s welcome Government **New Clause 65**- “Duty to report child sexual offences” but also request further clarity on the detail of how this provision will work in practice.
4. That MP’s speak in support of Government **New Clause 86**- “Creating purported image of an adult without consent”- highlighting the positives this amendment also brings for child protection.
5. That MPs highlight the need to deal with the challenges created by the surge of **Generative Artificial Intelligence** in creating child sexual abuse material online.

Background-

In June 2023, the Internet Watch Foundation started receiving its first reports from members of the public of child sexual abuse material which had been created using generative artificial intelligence. In July 2023, [the IWF called on the Prime Minister](#), to make this issue one of the top priorities for the planned AI Safety Summit, to be held at Bletchley Park.

Between September and October, the IWF used their proactive searching powers to conduct a [snapshot study](#) of one dark web forum and discovered over **20,000** AI generated images had been uploaded in just one month. Of these, **11,000** were selected by IWF analysts for further assessment and of these, nearly **3,000** images were found to be illegal. **2,562** images were assessed as criminal pseudo photographs and a further **416** assessed as criminal prohibited images.

These findings were presented at an AI Safety Summit fringe meeting, jointly hosted between the IWF and the Home Office, two days before the main AI Safety Summit at Bletchley Park. It led to **33 Government, Industry, NGOs and academics** signing a non-legally [binding voluntary pledge](#) to tackle the rise in child sexual abuse material in the age of Artificial Intelligence.

Since then, the IWF has been working with industry, Government, and other public safety organisations to ensure that UK laws are fit for purpose in response to the Generative AI challenge.

We have identified two legal loopholes that we are keen to close in the Criminal Justice Bill as it comes back for its Report Stage.

New Clause 25: Extending the existing offence of Possession of a Paedophile Manual:

Tabled by: Rt. Hon. Vicky Ford MP

Supported by: Rt. Hon. Suella Braverman MP, Rt. Hon. Sir Robert Buckland MP, Dame Diana Johnson, Sarah Champion MP, Kit Malthouse MP, Miriam Cates MP, Danny Kruger MP, Simon Jupp MP, Dame Margaret Hodge MP, Peter Dowd MP, Sally-Ann Hart MP.

The aim of this new clause is to expand the existing offence of possessing guides (so called Paedophile manuals) about abusing children to include guides on creating child sexual abuse content, including using Generative Artificial Intelligence or through Machine Learning.

Currently, Section 69 of the Serious Crime Act (2015), prohibits the creation, distribution, and use of paedophile manuals. However, it is only applicable as an offence if it relates to directions of the sexual abuse of real children and **specifically omits “pseudo photographs.”**

Section 69 of the Serious Crime Act (2015) **makes no reference to the offence of directing people to use technology such as text-to-image based Generative Artificial Intelligence or machine learning to create child sexual abuse material, or providing hints and tips on how to create these images.**

This is a gap in the current law which is already being used to exploit children.

A “sextortion” manual- Case Study:

On 12 February 2024, the Internet Watch Foundation, downloaded a text only manual from a public report it had received.

The manual was over **210 pages long** and contains detailed information and instructions on how to extort images and videos from teenagers.

It contained information on specific devices, apps, and websites to use to protect the perpetrator from detection.

In the guide, it discusses how to make initial requests for imagery, such as asking for images in a bikini or underwear for those unwilling to share nude images. It then goes on to discuss once these images have been provided, how nudifying AI technology can be used to remove clothing from underwear images to blackmail victims into sending nude images of themselves.

The manual states:

“It is possible to sextort some targets with photos of them wearing bras or underwear; however, if they do not care about you leaking their photos in bras or underwear after you have threatened them, then you can use an AI clothes remover on those photos and use that to threaten them. You could say something like, “it shows your face in the pic and you are basically nude, if I leak it, people will think it is you even though it is fake.”

New Clause 26: The offence of simulating sexual communication with a child:

Tabled by: Rt. Hon. Vicky Ford MP

Supported by: Rt. Hon. Suella Braverman MP, Rt. Hon. Sir Robert Buckland MP, Dame Diana Johnson, Sarah Champion MP, Kit Malthouse MP, Miriam Cates MP, Danny Kruger MP, Simon Jupp MP, Dame Margaret Hodge MP, Peter Dowd MP, Sally-Ann Hart MP.

The Law currently:

Under Section 15A of the Sexual Offences Act (2003) it is an offence to communicate sexually with a child. This includes for sexual gratification and if the communication is sexual or encourages the child to communicate sexually with the offender.

A communication is deemed to be sexual, if a reasonable person would, in all circumstances but regardless of any person's purpose, consider such communication to be sexual.

If found guilty of this offence on a summary conviction, the offender is liable to imprisonment of a term not exceeding the general limit of a magistrates' court, or a fine, or both.

On conviction on indictment, to an imprisonment term not exceeding two years.

What does this new clause do?

The purpose of New Clause 26 is to make it an offence to use, create or share online digital tools which simulate the offence of sexual communication with a child.

Evidence that supports the need for this change:

Within online paedophile communities there is always a desire to utilise technology to bring the fantasies of child sexual abuse closer to a reality.

The evolution of AI technology is seen as the ultimate solution in allowing them to feel close to the sensation of interacting with and abusing a real child as possible, without committing the act of physically abusing a child.

Some, argue that this could be a good thing in preventing child sexual abuse. This is something the Internet Watch Foundation and many of our partners **completely reject**.

Many of **these AI generated tools have been trained on real material involving real children and this type of interaction is far from a victim less crime**. We are very concerned that the development of AI Chatbots and the ease, speed, and quality at which text-to-image based Generative AI tools have been developed further lowers the bar to offending.

The [National Crime Agency estimates](#) that approximately **680,000-830,000 people**, between **1.3%** and **1.6%** of the adult population, in the UK pose some form of sexual threat to children.

Android and IOS Application stores have a plentiful supply of AI companion apps, with the three largest apps receiving well over a million downloads each.

Within minutes of downloading one of these popular apps, law enforcement operatives were able to have an interactive communication with an AI chatbot discussing the abduction, sexual abuse, torture, and murder of an 8-year-old girl. The chatbot also engaged in conversation around self-harm and encouraged the law enforcement investigator to cut themselves.

Through monitoring offender discussions online, some technically capable offenders are actively building AI chatbot companions for the purpose of having what they deem realistic paedophilic role plays with AI child avatars.

There are several reasons these AI chatbots are of concern:

1. It **normalises the sexual abuse of children** and encourages those with sexual thoughts about children to act on those urges. It **could and does lead to contact offending** in future, putting real children at risk of significant harm that will impact on them their whole life.
2. There is **no age verification process** in the availability of these AI chatbots. This means that **children have easy access** to these tools, putting them at significant risk of harm.
3. There are **significant concerns about how these tools are developed**, the data they are trained on, given how swiftly they move into extremely dark fantasies.

These services are also actively marketed to appeal to people seeking out sexualised content. Within the preview images available prior to download, the chatbot use phrases such as:

“At your service, anytime you wish”.

“This is your place where no one will judge you.”

The AI chatbot **technology needs to be more tightly controlled and regulated**, as Baroness Kidron has lobbied for in the other place, during the passage of the [Data Protection and Digital Information Bill, \(Amendment 291\)](#), and there is **certainly a role for app stores in whether these sorts of Apps should be available**;

BUT it is also important that people realise they have a **personal responsibility** not to engage in simulating the offence of sexual communication with a child.

At present, there is no responsibility on the individual, the entity or individual responsible for creating and sharing the tool. This amendment seeks to change this.

On 21 April, [the Guardian newspaper](#) reported how, a convicted sex offender, Anthony Dover, was ordered by a UK Magistrates court, in the first case of its kind, not to “use, visit or access” artificial intelligence tools without prior permission from police as part of his sexual harm prevention order imposed in February of this year.

This includes to text-to-image based generators, which can create lifelike pictures based on a written command and “nudifying” websites which can be used to create “deepfakes.”

Gov New Clause 65- Duty to report child sexual offences.

Tabled by: Rt. Hon. James Cleverly MP and Rt. Hon. Alex Chalk MP

What does the New Clause do?

This New Clause tabled by the Government, imposes a duty on persons engaging in a relevant activity in England to make a notification to the police or to a local authority if, in the course of that activity the person is given reason to suspect a child sexual offence may have been committed.

Background and support:

In October 2022, the [final report](#) of the Independent Inquiry into Child Sexual Abuse (IICSA) was published. It made [20 recommendations](#) as part of a package of reforms that were, it believed, required to ensure that institutional state failings are never repeated.

This Government amendment delivers on implementing recommendation 13 from the inquiry- Mandatory reporting of sexual abuse in certain circumstances, following the recent [public consultation](#) from the Home Office, which closed in November 2023.

The Internet Watch Foundation is part of the [IICSA \(Independent Inquiry into Child Sexual Abuse\) Changemakers](#), a group of 65 members including charities, individuals, people with lived experience of child sexual abuse, support services and groups that work on the frontline and have experience of preventing and tackling child sexual abuse.

The purpose of the group is to work together to bring about change. We want the support and protection of children and people who have been sexually abused to be a larger priority for the public and are focussed on ensuring Government delivers on the Independent Inquiry's findings.

In response to the Government's proposed amendment at report stage an IICSA Changemakers spokesperson, welcomed the move, but has also called for further clarity on how the provision will work in practice:

"Effective and timely reporting is a vital part of a well-functioning child protection system. But as the Government acknowledges, it remains important that children and young people have access to safe confidential spaces to speak about their experiences and to seek support. It is deeply disappointing that the detail of how that will be achieved remains unclear.

"It is vital that any mandatory duty to report abuse is matched with sufficient training and resources for professionals. Anybody who falls under this legal duty must be equipped with the skills they need to identify and respond appropriately to any concerns."

Further detail on the IICSA changemakers statement can be [read here](#).

Government New Clause 86- 'Creating purported sexual image of an adult'.

Tabled by: Rt. Hon. Alex Chalk MP

What does the new clause do?

This new clause creates an offence of creating a purported sexual image of an adult without consent.

Background:

The Government has [recently announced](#) changes to the Criminal Justice Bill that addresses the impact of “deepfake” technology that has been created without an adults knowledge or consent.

The Government correctly sets out that this offence only applies to adults as any imagery created of children would **already be deemed to be illegal** either under the Protection of Children Act (1978) or the Coroners and Justice Act (2009).

The IWF supports this move, as reported by a 404 media investigation [we have seen both Apple and Google remove](#) a number of AI generated apps that promised deepfake nudes from its app stores.

Whilst this amendment applies to adults, the removal of these apps and [seeing them disabled to public use in the UK](#) has huge benefits to the protection of children too. The two most prominent websites that have now been disabled to public access had **12 million** and **4 million** global visitors in the past month, with **500,000** and **50,000** users respectively coming from the UK.

We know that these applications are used to also create indecent images of children, often by children themselves. A case from [Spain last year](#) reported how **20 girls between the ages of 11 and 17** have come forward as victims of nudifying apps with **11 boys having been identified as being involved in either the creation of these images or their circulation** via platforms Telegram and WhatsApp.

This is against a backdrop of “normalised” image sharing between children. We know through [Ofsted’s recent review of sexual abuse in schools and colleges](#) that interviews with **900 children and young people**, revealed:

- that **90%** of girls and **50%** of boys had been sent unsolicited photos or videos, and
- **92%** of girls and **74%** of boys had endured sexist name calling.

This include being shown pornographic content and was typically found on platforms such as WhatsApp and Snapchat. Other forms of peer-on-peer abuse could include, upskirting, sexting and “youth produced imagery”.

For further information about this briefing please contact:

Michael Tunks, Head of Policy, and Public Affairs: mike@iwf.org.uk

Or

Bobbie Dennis, Policy, and Public Affairs Officer: Roberta@iwf.org.uk