CHILDLIGHT

Global Child Safety Institute

Legal challenges in tackling AI-generated child sexual abuse material across the 5 Eyes nations: Who is accountable according to the law?

UNITED KINGDOM

Authors:

Dr Konstantinos Kosmas Gaitis
Research Fellow (Policy & Legal Research), Childlight – Global Child Safety Institute, University of Edinburgh

Dr Chrystala Fakonti
Lecturer of Law, Glasgow Caledonian University

Dr Mengyao Lu
Research Fellow, Childlight – Global Child Safety Institute, University of Edinburgh

Mr James Stevenson
Technology-Facilitated CSEA Data Specialist, Childlight – Global Child Safety Institute, University of Edinburgh

Professor Deborah Fry
Personal Chair of International Child Protection Research, Childlight – Global Child Safety Institute, University of Edinburgh

Table of Contents

Abbreviations ... 3

Executive Summary ... 5

Introduction ... 10

Methodology ... 13

Legislative Review: UK ... 16

Conclusion and Recommendations ... 43

References ... 45

Abbreviations

AI – Artificial Intelligence

CA 2003 - Communications Act 2003

CCA Scotland 1982 - Civic Government (Scotland) Act 1982

CICA - Criminal Injuries Compensation Authority

CJA 1988 – Criminal Justice Act 1988

CJA 2009 - Coroners and Justice Act 2009

CJO NI 1988 - Criminal Justice (Evidence, Etc.) (Northern Ireland) Order 1988

CPS – Crown Prosecution Service

CSAM – Child Sexual Abuse Material

EEA – European Economic Area

EU – European Union

GCHQ - Government Communications Headquarters

GDPR - General Data Protection Regulation

ICMEC – International Centre for Missing & Exploited Children

IWF – Internet Watch Foundation

NCMEC – National Center for Missing and Exploited Children

OECD – Organisation for Economic Co-operation and Development

OFCOM - Office of Communications

OPA 1959 - Obscene Publications Act 1959

OSA – Online Safety Act

PCA 1978 – Protection of Children Act 1978

PCO NI 1978 - Protection of Children (Northern Ireland) Order 1978

SCA 2015 - Serious Crime Act 2015

SHPO - Sexual Harm Prevention Orders

SOA 2003 - Sexual Offences Act 2003

SOO NI 2008 - *Sexual Offences (Northern Ireland) Order 2008*

SRO - Sexual Risk Orders

UK – United Kingdom

Executive Summary

This study is among the first to critically review the regulatory context of the Five Eyes nations (UK, USA, Canada, Australia and New Zealand) on the topic of accountability around child sexual abuse material (CSAM) created via generative Artificial Intelligence (gen-AI). We examined this topic on a national, state and territory level in Australia; on a national level in New Zealand; on a federal and state level in the US; on a federal and provincial level in Canada; and lastly on a reserved and devolved level in Britain. We have identified key strengths, as well as weaknesses of the studied legislative contexts, which we selected due to their democratic political systems, their technologically advanced character, and their progressive legislative systems.

Legislation in the UK is divided between reserved and devolved matters. Reserved legislation is adopted by the Westminster Parliament. Devolved legislation is the legislation adopted by the Scottish Parliament or the Northern Ireland Assembly. Both levels of legislation were examined for this study covering all 4 nations of the UK (England, Northern Ireland, Scotland and Wales).

The legislation that is relevant for cases of AI-generated CSAM focuses on two types of indecent images. One type is indecent pseudo-photographs, meaning photographs as well as videos and films made by computer graphics that have a photo-realistic appearance, i.e., they look real. The other type covers prohibited pseudo-images that do not look realistic, such as drawings and cartoons or hentai and manga. Manga are Japanese comic books and graphic novels, while hentai are a type of Japanese manga and anime that portrays sexualised content, storylines and characters. There is concern in some parts of the world, such as the UK, that when these types of imagery present children in a pornographic, offensive or otherwise obscene way, focus on children's private parts or display prohibited acts including children, there is a risk that they may be normalising child abuse and encouraging harmful behaviour. Notably, these concerns are not shared on a global scale and research on the matter is not yet robust.

We found that there is good coverage around a series of offences with regards to pseudo-photographs, i.e., the acts of making, taking, possessing, and disseminating pseudo-photographs are all covered, irrespective of the technology used, thus covering cases of generative AI or deepfakes. This is evidenced by the first emerging case in England, where an offender who created CSAM using generative AI was arrested, charged, and sentenced to 18 years in prison. In this instance, and as per a recent BBC report, the Crown Prosecution Service, warned that those thinking of using AI "in the worst possible way" should be "aware that the law applies equally to real indecent photographs and AI or computer-generated images of children" (Gawne, 2024). That said, the law is silent on whether the criminalisation of indecent pseudo-photographs of children extends in cases of fictitious children.

However, this protection tends to be less efficient with regards to non-realistic images, including cartoons, manga and drawings. While possession and dissemination are criminalised for real and fictitious children, the act of making such imagery is not criminalised in England and Wales. The largest gap in protection with regards to the above imagery exists in Scotland, as the making and possession of indecent non-realistic images in Scotland is not criminalised. The nation that seems to have the most robust legislative framework against all acts related to indecent non-realistic images is Northern Ireland.

Another gap that exists across the UK is around the possession of paedophile manuals, meaning guides on how to sexually abuse children. Existing legislation does not apply in cases of possessing a paedophile manual that specifically instructs on how to misuse generative AI to produce CSAM. Ongoing UK legal reforms are targeting this specific gap in the legislation (Home Office, 2025; see section 64 Crime and Policing Bill). In Scotland, we found no legislation on paedophile manuals. Arguably, this may heighten the risk of widespread dissemination of manuals containing instructions on how to sexually abuse and/or exploit children.

There has been no case law, i.e., court cases, on criminal liability for omissions (the failure to perform a legal duty when one can do so) in cases of AI-generated CSAM, but there may be room to argue that it is possible for such liability to arise in the case of a close personal relationship and assumed responsibilities, i.e., in relation to a child's parent(s) or guardian(s).

Notably, the UK recently adopted the Online Safety Act, which places new duties on social media companies and search service providers to protect children and other vulnerable adult users online. The Act applies specifically to user-to-user services (e.g. social media, photo or video-sharing services, chat services and online or mobile gaming services); search services; and to businesses that publish or display pornographic content (OFCOM, 2025). The regulation of harmful content to children is a top priority for the Online Safety Act. Therefore, and among other legislated duties, the law mandates the abovementioned companies to remove illegal content, such as CSAM and even if this has been created by generative AI, and take steps to prevent users from encountering it (OFCOM, 2024).

From a civil perspective, there is no specific legislation or case law in the UK that directly addresses this issue, leaving a significant gap. However, AI-generated CSAM seems to fall under the protective remit of the Data Protection Act 2018.

There is the ability to claim compensation in the UK with regards to CSAM created via gen-AI technologies that includes figures modelled after real, identifiable children via a number of pathways (a civil claim, privacy infringement, compensation order via criminal courts, and, much less likely, via the Criminal Injuries Compensation Scheme [CICA]). However, the liability for AI-CSAM, i.e., the question “who is the author of AI” remains currently unclear under existing legislation across the UK.

What also became evident from the above analysis is the fact that the UK lacks a targeted AI industry regulation, like the one that was recently adopted in the European Union in the form of the EU’s AI Act. There seem to be no plans at the moment for a standalone UK AI Act.

Lastly, a more recent legal reform concerns AI tools. More specifically, the UK is planning to make it illegal to possess, create or distribute AI tools designed to create CSAM, with a punishment of up to five years in prison (Home Office, 2025; see s63 Crime and Policing Bill on CSA Image Generators).

Based on these findings, the following recommendations are made for the UK:

Recommendation 1. Update the law to clearly criminalise all acts relevant to pseudo-photographs that depict purely fictitious children, i.e., making, taking, disseminating and possessing such material.

Recommendation 2. The Scottish Government should introduce legislation to criminalise all acts relevant to non-photographic indecent images of children, i.e., making, taking, disseminating and possessing such material.

Recommendation 3. Amend existing legislation that is in force in England and Wales to criminalise the making of indecent non-photographic imagery of children

Recommendation 4. Update UK legislation on paedophile manuals to make it applicable on pseudo-photographs; and on criminal responsibility for software creators. As stated above, reforms on the matter are currently underway.

Recommendation 5. Strengthen legislative protection against all forms of paedophile manuals in Scotland.

Recommendation 6: Amend language used in UK-wide legislation to make it more inclusive, wide and encompassing

Introduction

Child sexual exploitation and abuse (CSEA) is considered a violation of children's rights and dignity (Ngo, 2021). A "widespread, worldwide issue of concerning magnitude" that affects both girls and boys (Simon, Luetzow & Conte, 2020: 2). CSEA may entail a series of negative effects for victims, which can impact their physical, mental or psychological health, their emotional wellbeing, social skills and interpersonal relationships, economic status, as well as vulnerability to future victimisation (Fisher et al., 2017). Within this, technology and related platforms or online environments are considered spaces which can be protective, but also pose significant risks to children's safety, increasing their vulnerability to CSEA victimisation (Simon, Luetzow & Conte, 2020). This vulnerability to victimisation is considered to be higher for children than adults (Quayle, 2016).

The rapid development of technology has led to the birth of new, immersive forms of technology, which are usually grouped under the umbrella term "eXtended Reality" (XR) (Huang, 2022). Prominent among these emerging technologies is Artificial Intelligence (AI), defined widely by Bahoo, Cucculelli and Qamar (2023: 1) as "the system's ability to interpret data and leverages computers and machines to enhance humans' decision-making, problem-solving capabilities, and technology-driven innovativeness". As such and following the increasing dissemination of child sexual abuse material (CSAM) noticed across the clear and dark web, AI can prove to be a valuable tool in the efforts against CSEA by allowing the invention of detection intelligence algorithms that will use deep-learning techniques as a method of accurate detection of CSAM online (Lee et al., 2020; Ngo, McKeever & Thorpe, 2023). However, AI can also be misused by offenders to create CSAM with varying levels of realism that can often be hardly distinguishable from real-life material (Internet Watch Foundation, 2023). Irrespective of whether AI-created CSAM involves artificial children or children modelled after real-life children, there is widespread concern that it can be a pathway to higher levels of CSEA offending that may include the sexual exploitation and abuse of children in real life (Internet Watch Foundation, 2023). As such, it requires a robust and clear legislative response, particularly with regards to accountability over AI-created CSAM. This call comes amidst a hotly contested debate, with some stakeholders promoting notions that CSAM created via generative AI does not hurt real children or that it may also serve to divert potential offenders from sexually exploiting and abusing real children, while others fear that generative AI-created CSAM may be the first step on a pathway towards higher offending in CSEA with real children (Internet Watch Foundation, 2023).

Based on the above, examining the existing legislative context of the Five Eyes countries, which comprise Australia, Canada, New Zealand, the United Kingdom (UK) and the United States of America (USA), becomes crucial in order to assess the readiness of their regulatory frameworks against the phenomena of AI-created CSAM and AI-facilitated child sexual exploitation and abuse. These countries have a long history of association dating back to 1956 (Weaver & Roseth, 2024). A recent study provided a review of the legal challenges that AI-generated CSAM presents in the context of Europe. Similar to the present study, this research looked at legal frameworks concerning both the creation and generation, as well as the distribution of that child sexual abuse material (Parti & Szabo, 2024). The five countries have been selected due to their democratic and open political systems, their high levels of technological advancement and literacy, as well as their progressive and advanced legislative systems, which often serve as the regulatory blueprints for other countries across the globe to model their legislation after. It also assists in forecasting the potential technological developments that have yet to be created or alternatively used in the sexual harm of children. By identifying and helping to shore up any gaps in legislation now, it will be much easier in the future to address technology-facilitated CSEA (TF-CSEA) through the use of AI. It is especially timely as four of the five included countries are in the process of ratifying or drafting legislation to address online environment safety. The United Kingdom and Australia are in the process of implementing the respective Online Safety Acts, with Canada and the United States currently working on multiple pieces of legislation to address safety online (Ness et al., 2023). The capacity of AI-driven CSAM and child sexual abuse and exploitation will only increase with time as technology continues to develop (Parti & Szabo, 2024). It is important that legislation in countries known for combatting TF-CSEA is prepared for this. As such, it is necessary for this study to review the full breadth of legal coverage for crimes committed against children using any type of AI.

Methodology

Given that XR environments, and first and foremost AI, constitute a new and evolving field of technology, we anticipate gaps in legislation across the Five Eyes nations on the matter of accountability over AI-generated CSAM. To examine our research hypothesis, we decided to conduct a legislative review of relevant laws and case law across the Five Eyes countries (USA, UK, Canada, Australia, New Zealand).

The review and analysis of the emerging pieces of legislation and caselaw was informed by the "black-letter law" approach (McConville & Chui, 2007), also known as doctrinal legal research method. Using this method, we gathered legal rules found in primary sources, such as statutes, case law, regulations, and proposed bills, and identified underlying themes or systems of application related to each source to develop a descriptive and detailed analysis of the effectiveness of existing laws, identify ambiguities and gaps, and suggest necessary legal reforms. This approach focuses on the letter of the law rather than on the spirit of the law, and is therefore taking a more "literal approach to reading the law", as Wright (2018: 30) points out. By critically analysing primary and secondary legal sources, the aim of this approach is to restrict the number of possible outcomes, thus succinctly summarising and clarifying what the law instructs in a more systematised and narrower way than socio-legal analyses, which tend to look more at the broader societal, political and policy context of legislation (Wright, 2018). The identification of themes in our legislative analysis is guided by our aforementioned research hypothesis and research questions.

More specifically, we reviewed laws and case law from the Five Eyes countries on the topic of accountability with regards to generative-AI CSEA/CSAM. Legislation and case law was eligible for inclusion, if they focus on any area that intersects with accountability for CSEA/CSAM and particularly with regards to generative AI software; or if they defined concepts that are applicable and useful for phenomena of AI-generated CSAM (e.g. case law defining the concept of obscenity). There was no defined search period, as any legislation or caselaw that can be applicable on the study topic will be included. All legislative and caselaw sources were in English given that all countries studied are Anglophone nations.

To identify relevant legislations and cases across the UK, we conducted an initial search of Lexis+UK/Lexis Nexis, Practical Law, Google Scholar, Google and Westlaw UK; utilised official Government sources; and searched on local court and prosecution services' websites (e.g. Crown Prosecution Service [CPS] in England etc.).

To identify potential law reforms as well as updates on the most recent cases, we conducted internet searches, consulted media sources and obtained discussion papers or reports from the relevant Government agency websites. Supplementary materials, including press releases, news articles and policy reports, were identified through standard search engine queries and databases such as the Koons Family Institute/ International Centre for Missing & Exploited Children (ICMEC) database and the Organisation for Economic Co-operation and Development (OECD) database.

Lastly, networking with and consulting our extensive network of experienced colleagues located across the UK crucially assisted us in locating further legislations or caselaw on the matter that we were not able to obtain via the above methods.

All identified legislations were collated and organised via Excel spreadsheets and then analysed. Traditional methods of selection process did not apply here, given that both the existence and non-existence of relevant legislative provisions or caselaw on the studied topic have equal research value and led to important conclusions regarding the strengths and weaknesses of said legislation and regulatory frameworks of the 5 studied nations.

Data was extracted using a data extraction tool developed by the research team (https://osf.io/as83r/files/osfstorage/67851f0aaeb11fe8762f3f18). The data extracted included specific details about legislative definitions, provisions regarding accountability and other key findings relevant to the review questions. More specifically, the data extraction tool contained themes such as:

- Definitions: How reserved, devolved, federal, state, and provincial laws define terms such as “pseudo-photographs”, “indecent material”, "child pornography",[1] "obscene material," and related offenses, with a particular focus on computer-generated content.
- Accountability Provisions: Mechanisms by which individuals, platforms, and third parties are held accountable for producing, hosting, or distributing AI-generated CSAM.
- Civil Remedies: Available remedies for victims seeking compensation, particularly where AI CSAM is involved.
- Legislative Gaps: Identification of areas where legislation lacks clarity, such as the legal status of using real CSAM in AI training datasets.

This structured approach ensured a comprehensive review of current legal frameworks while highlighting areas for potential reform to meet the challenges posed by advancements in AI technology. We examined 30 pieces of legislation and 25 cases for the UK context.

[1] Childlight follows the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. The terms ‘child abuse’, ‘child prostitution’, ‘child pornography’ and ‘rape’ are used in legal contexts.

Legislative Review: UK

Indecent (pseudo-)photographs children

To begin, the *Protection of Children Act 1978* (PCA 1978), in s1, criminalises 4 different acts in a broad, tech-agnostic way, covering a wide remit of conducts in relation to indecent photographs or pseudo-photographs of children. These include the:

1. Taking or making
2. Distributing or showing
3. Possessing with a view to distribute or show
4. Publishing or causing the publication of "any advertisement that is likely to be understood as conveying that the advertiser distributes or shows such indecent photographs [or pseudo-photographs], or intends to do so."

Regarding punishment, this would be imprisonment, fine or both.

Examining the abovementioned types of offences more closely and as the Crown Prosecution Service (CPS) claims in its guidance, the act of *making* has been interpreted widely in courts. More specifically, "to make" indecent (pseudo-)photographs has been interpreted in caselaw to include:

- opening image(s) attached to an email (R v Smith; R v Jayson [2003] 1 Cr. App. R. 13)
- downloading an image (R v Smith; R v Jayson [2003] 1 Cr. App. R. 13)
- storing an image (Atkins v DPP; Goodland v DPP [2000] 2 Cr. App. R. 248)
- accessing a pornographic website, where relevant indecent material appeared as pop-up on screen (R v Harrison [2008] 1 Cr. App. R. 29)
- receiving an image via social media

- live-streaming indecent material (CPS, 2024a)

CPS (2024a) details the various uses of technologies such as peer-to-peer file sharing, social media and messaging applications or chat rooms, where any of the above acts can be committed. CPS (2024a) instructs that even if material was deleted, is located in unallocated computer space and is not retrievable, provided that the downloading of the image or its transfer is proven, the offence of making an indecent (pseudo-)photograph is still committed.

The act of *taking* requires intention and purpose (*R v DM [2011] EWCA Crim 275*2). Same with regards to *possession*, where distribution must be within the defendant's intentions (see *R v Dooley [2006] 1 Cr. App. R. 21*). For incidences of simple possession (no purpose of dissemination), the *Criminal Justice Act 1988* (*CJA 1988*) applies instead. In s160, the *CJA 1988* criminalises the possession of an indecent (pseudo-)photograph of a child, punishable as per s160(2A)-(3) on indictment of an offence to imprisonment for up to five years or a fine, or both; and on summary conviction to imprisonment for up to six months or a fine or both.

When offences are committed by corporations, s3(1) applies:

> *"Where a body corporate is guilty of an offence under this Act and it is proved that the offence occurred with the consent or connivance of, or was attributable to any neglect on the part of, any director, manager, secretary or other officer of the body, or any person who was purporting to act in any such capacity he, as well as the body corporate, shall be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly."*

S3(2) extends the above provision in cases where the affairs of the corporation are managed by its members and the case concerns acts and defaults of a member in connection with their conducting management as if they were directors. Corporate responsibility is thus structured broadly and can leave scope for the criminal liability of corporations where offences occur through their actions or omissions when there is consent, connivance or neglect. Still, there needs to be caselaw on the matter with regards to gen-AI CSAM to establish how this corporate responsibility is applied in practice and if it can be applied against creators of gen-AI technologies.

As regards what is included under the term “photographs”, S7(2)-(5) defines that this includes films, video-recordings and photographs comprised in a film; negative and positive versions; data stored on a computer disc or by other electronic means capable of conversion in a photograph; tracing or other image made by electronic or any other means deriving from a (pseudo-)photograph. S7(7)-(9) defines what a pseudo-photograph is: an image made by computer graphics or any other methods, which maintains a photographic appearance. In general, it is accepted that s7 *PCA 1978* widens the scope of the law (and correspondingly of the *CJA 1988*) to encompass films and video-recordings, tracings of a picture and data which could be turned into a photographic image.

As regards the concept of indecency of the said material, this undergoes a case-by-case basis examination, with reference to an objective test, considering the depicted child’s age and concentrating on the indecency of the material (see *R v Neal [2011] EWCA Crim 461*; *R v Owen (1988) 86 Cr. App. R. 291*; *R v Graham-Kerr (1989) 88 Cr. App. R. 302*; *R v Smethurst [2002] 1 Cr. App. R. 6*).

Lastly, and with regards to possible defences against charges brought for the offences in s1(1)(b) and s1(1)(c) PCA 1978 and s160 CJA 1988, we firstly have the defence for legitimate reason, as per s1(4)(a) *PCA 1978* and s160(2)(a) *CJA 1988*. In s1(4)(b) *PCA 1978* and s160(2)(b) *CJA 1988*, the law allows for the defence of lack of awareness, where the defendant must prove that they did not see the photographs and did not know or have any cause to suspect them to be indecent. Marriage or civil partnership is another defence jointly mentioned in s1A *PCA 1978* and s160A *CJA 1988,* for photographs of children over 16 who are married to or in civil partnership with the defendant and have consented to the photographs in question. S1B(1)(a)-(c) *PCA 1978* provides exception for criminal justice workers, Secret Service and Government Communications Headquarters (GCHQ) employees from criminal proceedings and investigations with regards to the offence listed specifically in s1(1)(a) (making an indecent photograph or pseudo-photograph of a child) if they prove that the making of the photograph was necessary for "the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings, in any part of the world". A similar defence has been extended following the enactment of the *Online Safety Act 2023* (*OSA 2023*) to Office of Communications (OFCOM) members for cases where the photograph or pseudo-photograph is made for the purposes of OFCOM's exercise of any of their online safety functions, as per s1B(1)(d)(i) and (ii) *PCA 1978*. The same defence is afforded for OFCOM members, as per s213 *OSA 2023*, with regards to publication of obscene articles. S160(2)(c) *CJA 1988* mentions the unsolicited photographs defence with regards to the offence listed in s160(1) *CJA 1988* specifically, and for those defendants who can prove that the photograph was sent to them without any prior request made by them or on their behalf and that they did not keep it for an unreasonable time, as judged on a case-by-case basis (CPS, 2024a).

The *Protection of Children (Northern Ireland) Order 1978* (*PCO NI 1978*), sets out similar provisions for indecent (pseudo-)photographs in Northern Ireland. S8 combined with s20(2) of the *Interpretation Act (Northern Ireland) 1954* sets corporate liability:

> *"notwithstanding and without prejudice to the liability of that body, any person who at the time of such commission was a director, general manager, secretary or other similar officer of that body or was purporting to act in any such capacity shall be liable to be prosecuted as if he had personally committed that offence*

> *and shall, if on such prosecution it is proved to the satisfaction of the court that he consented to, or connived at, or did not exercise all such reasonable diligence as he ought in the circumstances to have exercised to prevent the offence, having regard to the nature of his functions in that capacity and to all the circumstances, be liable to the like conviction and punishment as if he had personally been guilty of that offence."*

The offence of simple possession is included in the *Criminal Justice (Evidence, Etc.) (Northern Ireland) Order 1988* (*CJO NI 1988*). In s15, the *CJO NI 1988* criminalises the possession of an indecent pseudo-photograph of a child, punishable by fine and/or imprisonment. The defences of legitimate reason; lack of awareness; unsolicited sending of the photos to the defendant; and consensual photographs in the context of marriage with a child aged 16 and above apply here too (see ss.15-16).

In Scotland, we have the *Civic Government (Scotland) Act 1982* (*CCA Scotland 1982*). Similarly to *PCA 1978* and *PCO NI 1978*, the acts of taking, distributing, possessing with a view to distribute and publishing of indecent photographs of children are criminalised, as per s52(1), are punishable with imprisonment and/or fine. S52A also criminalises the simple possession of children's indecent photographs. The offence extends to pseudo-photographs, which are defined in a similar fashion to *PCA 1978* and *PCO NI 1978*. The acts of making or possessing have been equally interpreted widely in Scotland, as mentioned above in the analysis of PCA 1978. Similar defences of legitimate reason, lack of awareness, marriage, OFCOM membership apply.

The legislation on indecent children's (pseudo-)photographs, namely *PCA 1978*, *PCO NI 1978* and *CCA Scotland 1982*, does not make explicit reference to the criminalisation of (pseudo-)photographs depicting imaginary/fictitious children. Given the intention of the legislators on the matter, which is the increase of child protection and safety in a way that is broad and encompassing of technological developments, the law should be interpreted in a way that even pseudo-photographs of imaginary children are covered by it. Still, a possible updating of the law on the matter to succinctly state the inclusion of imaginary children under its remit could be helpful, as there can be valid arguments for the opposing view.

Overall, we found that there is good coverage around a series of offences with regards to pseudo-photographs, i.e. the acts of making, taking, possessing, disseminating, which are all covered for pseudo-photographs irrespective of the technology used, thus extending to cases of generative AI, deepfakes or any other technology used to create such pseudo-material. The legislation on indecent children's (pseudo-)photographs seems to be working well for the time being, as evidenced by the fact that we have already witnessed the first emerging case in England, where an offender who created CSAM using generative AI was successfully arrested and charged for that (Gawne, 2024).

Indecent non-photographic (pseudo-)images of children

With regards to images that do not have a photographic and therefore photorealistic appearance, the *Coroners and Justice Act 2009* (*CJA 2009*) applies with territorial extent that covers England, Wales and Northern Ireland (s181), but not Scotland, creating a gap for that nation. As per s65 *CJA 2009*, the law covers moving or still images. S62(1) *CJA 2009* criminalises only the possession of these prohibited images, even if they depict purely imaginary children [s65(8)].

The defences outlined in s64 *CJA 2009* for offences under section 62(1) CJA 2009 include some of the defences that we saw above in *PCA 1978* and *CJA 1988* and more specifically the legitimate reason, lack of awareness and unsolicited images defences.

Now, as per s62(2), (3), (6) and (7) these non-photographic images must be pornographic; grossly offensive, disgusting or generally obscene, and either focusing “solely or principally on a child's genitals or anal region” or portray the following acts:

- intercourse or oral sex of a person with or in the presence of the child
- masturbation by, of, involving or in the presence of the child
- penetration of the child’s vagina or anus with either the part of a person’s body or anything else
- penetration, in the presence of a child, of the vagina or anus of a person with a part of a person's body or with anything else
- the performance by a child of an act of intercourse or oral sex with an animal (whether dead or alive or imaginary)
- the performance by a person of an act of intercourse or oral sex with an animal (whether dead or alive or imaginary) in the presence of a child.

Punishment includes imprisonment, fine or both. Powers of entry, search and seizure apply too (s67 *CJA 2009*).

Regarding the difference between photographs/pseudo-photographs on one hand, and still/moving images that come under *CJA 2009* on the other, according to CPS (2024a), the latter term covers non-photographic images, such as “Computer-Generated Images (CGIs), cartoons, manga images and drawings”, i.e. images that do not look photorealistic. Manga are Japanese comic books and graphic novels, while hentai are a type of Japanese manga and anime that portrays sexualised content, storylines and characters. There is concern in some parts of the world, such as the UK, that when these types of imagery present children in a pornographic, offensive or otherwise obscene way, focus on children’s private parts or display prohibited acts including children, there is a risk that they may be normalising child abuse and encouraging harmful behaviour. Notably, these concerns are not shared on a global scale and research on the matter is not yet robust.

Given the above, the coverage for pseudo-CSAM which takes the form of a pseudo-photograph of a child (photorealistic) is more encompassing compared to the respective coverage for indecent still or moving pseudo-images that do not appear to look like photographs (non-photorealistic), due to the gap with respect to the making and distribution of still and moving (pseudo-)images of children.

Still, the UK-wide *Obscene Publications Act 1959* (*OPA 1959*) has to be factored in as well, specifically with regards to still/moving pseudo-images of children (real or imaginary). Looking at the *OPA 1959*, this act contains a very broad and therefore encompassing conceptualisation of what an "obscene article" is according to s1(1): an article that may "deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it." (see also *Anderson [1972] 1 QB 304*). The concept of (moral) depravity has been analysed further in *R v Penguin Books Ltd* (also known as *The Lady Chatterley Trial*): "To deprave means to make morally bad, to pervert, to debase or to corrupt morally. To corrupt means to render morally unsound or rotten, to destroy the moral purity or chastity, to pervert or ruin good quality, to debase, to defile". As CPS (2019) states if the article contains "sexual / pornographic activity which involves the commission of a crime" that renders it obscene. Given the criminalisation of indecent still or moving images of children under *CJA 2009*, we may conclude that disseminating this prohibited material, even if created via gen-AI technologies and irrespective of whether this concerns real or purely imaginary children, will be considered an offence under *OPA 1959*.

The law includes a set of defences for those charged with an offence: the defence of public good in s4(1) “if it is proved that publication of the article in question is justified as being for the public good on the ground that it is in the interests of science, literature, art or learning, or of other objects of general concern”; and, as per s2(5), if the person “proves that he had not examined the article in respect of which he is charged and had no reasonable cause to suspect that it was such that his publication of it would make him liable to be convicted of an offence against this section”.

This leaves the act of making prohibited (pseudo-) images of children uncovered by legislation, which may be covered for the nation of Northern Ireland through the *Sexual Offences (Northern Ireland) Order 2008* (*SOO NI 2008*): s38(1A) - intentionally causing or inciting an underage person to be involved in the recording or streaming or other transmission of an indecent image of the child); s39(1A) - intentionally controlling any of the activities of a child relating to the child’s involvement in the recording or streaming or other transmission of an indecent image of them; and s40(1A) - intentionally arranging or facilitating the involvement by a child in the recording or streaming or other transmission of an indecent image of that child. In s2(7), the act defines the concept of image in a very wide and encompassing way, covering non-photographic images of fictitious children too [see s2(8)], thus being applicable in cases of gen-AI CSAM. The same coverage is not found for England, Wales and Scotland, where the act of making indecent still/moving images of children is not covered.

Deepfakes

Another technological development tightly connected with gen-AI is deepfakes. Deepfake pornography is the falsification of sexual imagery and videos by the addition of the facial features of an unsuspecting person taken from a nonsexual image of theirs (Ryan-White, 2022). A recent popular manifestation of deep fake pornography is the so-called “nudify apps”. These apps allow users to create and then potentially share material that depicts real, identifiable people who via the application of AI filters or editing tools are made to appear nude. The AI used in these apps operates often on deep learning, which involves training AI on large datasets of images to accurately simulate and achieve the intended results.

This offence is covered to an extent in legislation across the UK. Regarding children, the abovementioned legislation on the creation/making, taking, possession and dissemination of indecent pseudo-photographs of children applies in the case of deep fakes and nudify apps as well, providing adequate coverage for children. Regarding adults, s66B Sexual Offences Act 2003 (*SOA 2003*), as added by s188 of the *OSA 2023*, instructs that A commits the offence if they “intentionally share photograph or film which shows, or appears to show, another person (B) in an intimate state” without B’s consent; or A does so to cause B “alarm, distress or humiliation” again without B’s consent; or does so for the purpose of obtaining sexual gratification again without B having consented; or threatens to proceed to the above act of sharing. In Scotland, the *Abusive Behaviour and Sexual Harm (Scotland) Act 2016* lists a similar offence to the above covering non-consensual sharing of deepfake pornography in s2. In Northern Ireland this offence is listed in s51 of the *Justice Act (Northern Ireland) 2016*, as this was amended by s6 of the *Justice (Sexual Offences and Trafficking Victims) Act (Northern Ireland) 2022*. However, with regards to adults portrayed in material created via deep fake technology, there is a legislative gap regarding the making/creating and the possession of such material (e.g. material created via nudify apps), which is currently not criminalised. The UK government has announced its plans to make creating sexually explicit “deepfake” images a criminal offence. New offences for the taking of intimate images without consent and the installation of equipment with intent to commit an offence will also be created.

Notification and orders

The *Sexual Offences Act 2003* lists a number of different types of orders which serve as tools for effective law enforcement against a number of offences cited above. As per Schedule 3 *SOA 2003*, these orders apply for the following relevant offences: “an offence under section 1 of the *PCA 1978* (indecent photographs of children)”; “an offence under s170 of the *Customs and Excise Management Act 1979* (penalty for fraudulent evasion of duty etc.)” which is “in relation to goods prohibited to be imported under s42 of the *Customs Consolidation Act 1876* (indecent or obscene articles), if the prohibited goods included indecent photographs of persons under 16”; “an offence under section 160 of the *CJA 1988* (c. 33) (possession of indecent photograph of a child)”; “an offence under section 66B(3) *SOA 2003* (sharing intimate photograph or film for purpose of obtaining sexual gratification)”; “an offence under Article 3 of the *PCO NI 1978* (S.I. 1978/1047 (N.I. 17)) (indecent photographs of children)”; “an offence under Article 15 of the *Criminal Justice (Evidence, etc.) (Northern Ireland) Order 1988* (S.I. 1988/1847 (N.I. 17) (possession of indecent photographs of children)”.

The orders that may be imposed for the abovecited offences include first and foremost notification requirements, commonly referred to as the “sex offenders’ register” (see s80 onwards *Sexual Offences Act 2003*). Under the *Sexual Offences Act 2003 (Notification Requirements) (England & Wales) Regulations 2012*, since August 2012 those subject to notification requirements are also required to notify police about details such as foreign travel; notify weekly of their residing place if they do not have a main residence; if they are living in a household with a minor; and bank account and credit card details (for the purposes of tackling engaging with online CSAM); and passport details or other identity documentation.

Another tool is the Sexual Harm Prevention Orders (SHPO) for England and Wales against a person who is found not guilty for a Schedule 3 offence by reason of insanity or found to be under a disability and to have done the act charged, or cautioned etc. (s103A). Considerations of necessity, proportionality, effective policing and risk minimisation need to be made for an SHPO to be imposed and the Order must include the least possible prohibitions that are necessary for the protection of the public or children, as was also mentioned in *R v Smith and Others* [2011] EWCA Crim 1772. The order may include prohibitions about engaging in certain professions (e.g. home tutor) or around engaging in certain activities online.

Sexual Risk Orders (SROs) for England and Wales can be also imposed upon the defendant if they have “done an act of a sexual nature as a result of which there is reasonable cause to believe that it is necessary for a sexual risk order to be made” (s122A). A key difference between SHPOs and SROs, is that the latter do not require a criminal conviction. The lowering of the standard of proof from the criminal standard to the standard of balance of probabilities for both SHPOs and SROs, as brought by the *Police, Crime, Sentencing and Courts Act 2022*, is a controversial change that aims to increase public protection, but simultaneously renders the position of the defendant considerably more precarious when compared to their pre-amendment status. Similar orders exist in Scotland and Northern Ireland too.

Further Offences

Serious Crime Act 2015 (*SCA 2015*), in s69, criminalises the possession of a paedophile manual, i.e. “any item that contains advice or guidance about abusing children sexually” and is punishable with imprisonment and/or fine. As s69(8) explains “abusing children sexually” includes offences under *PCA 1978* or *PCO NI 1978* involving indecent photos of children, but not pseudo-photographs. This leaves a gap as regards the exchange of paedophile manuals on how to misuse gen-AI software to produce gen-AI CSAM. As the Internet Watch Foundation (IWF, 2024) states, this gap could be corrected by a relevant addition made to *Serious Crime Act 2015*. Ongoing Westminster-based legal reforms are targeting this specific gap in the legislation (Home Office, 2025; see section 64 Crime and Policing Bill). With regards to Scotland, we did not find any specialised legislation which creates a similar targeted offence in the matter. This creates a regulatory gap for Scotland.

The *Anti-social Behaviour, Crime and Policing Act 2014*, in s116(1), instructs that police may issue a notice to the owner, operator or manager of a hotel that the officer reasonably believes has been or will be used for the purposes of child sexual exploitation, or conduct that is preparatory to, or otherwise connected with, child sexual exploitation. This according to s116 8(b) includes the commission of offences around indecent photographs of children (s1 PCA 1978). The law does not explicitly mention pseudo-photographs, therefore there could be scope here for adding this provision in to cover those cases where an online user can e.g. exploit the hotel’s WIFI for commission of an offence relevant with gen-AI CSAM.

Lastly, the *SOA 2003* details a few offences which might be applicable in the wider context of gen-AI CSAM. S48 lists the offence of causing or inciting the sexual exploitation of a child in any part of the world. S49 lists the offence of intentionally controlling any of the activities of a child in relation to sexual exploitation in any part of the world. S50 includes the offence of intentionally arranging or facilitating the sexual exploitation of an underage person in any part of the world. Now, crucial to the wide and encompassing character of s48-

50 is s51 which gives a very broad definition of the term “sexual exploitation” as updated by s176 of the *Policing and Crime Act 2017*: an underage person is sexually exploited if—"on at least one occasion and whether or not compelled to do so, B offers or provides sexual services to another person in return for payment or a promise of payment to B or a third person, or an indecent image of B is recorded [or streamed or otherwise transmitted]; and ‘sexual exploitation’ is to be interpreted accordingly”. This concerns cases where the offender is offering financial advantages to an underage person for the recording of sexual activities to create indecent imagery. The law does not mention pseudo-images specifically, as cases would usually entail payment for the creation of real photographs/imagery; however, the addition of pseudo- here would help extend the scope of this legislation to cover cases where children might enter exploitative relationships where for the exchange of money they can send non-indecent imagery to prospective offenders, who can then use gen-AI software to create artificial CSAM modelled after the said real child.

Communications and service providers – The *Online Safety Act 2023*

There exists legislation dealing with communications that might be relevant here. The *Communications Act 2003* (CA 2003) is central in this area. OFCOM was initially established by the *Office of Communications Act 2002*, but received its full authority and functions from the *CA 2003*. The Act is also important because it defines electronic communications networks and services, in s32. The *CA 2003* lists two summary offences under section 127(1) (sending a message which is grossly offensive, indecent, obscene, or menacing via a public communications network); and, under section 127(2)(c) (persistently making inappropriate use of a public communications network). Alternatively, and in case that this dissemination is by non-electronic means (e.g. print off a photographic piece of gen-AI CSAM and disseminate this via the post) to people with the intention to cause them distress or anxiety is well covered under s1 of the *Malicious Communications Act 1988.* The importance of this law is exactly its wider remit, which spans over non-electronic means of communications. The law cites that the communications must have been "indecent" or "grossly offensive", which are ordinary English words, as per *Connolly v DPP [2007] 2 ALL ER 1012*. Arguably, gen-AI CSAM does fit under these concepts and the law applies, provided that dissemination was done by the sender with at least one of its purposes being to cause recipients distress or anxiety.

Given the emphasis placed by *CA 2003* in "public electronic communications network", it is worth noting that this was defined as "a service provided for and funded by the public, for the benefit of the public" (*Director of Public Prosecution v Collins [2006] 1 WLR 2223*) The term has been interpreted widely in caselaw to encompass the internet, mobile phone networks widely available to the public and social media platforms which use internet for their operation, such as WhatsApp (see *DPP v Bussetti [2021] EWHC 2140 (Admin)*). As CPS (2024b) explains "it is not necessary to show the message was addressed to, or received by, another person. The actus reus of the offence is complete when the message is sent", citing *DPP v Collins [2006] UKHL 40*, as well as *DPP v Kingsley Smith [2017] EWHC 359 (Admin)*. Therefore, posting, re-posting and any other act of sharing said message is included here. Generally posting something on social media (e.g. Twitter/X or a blog), even if it is not directed towards a certain group or individual, even if the message can only be retrieved by searching it specifically, or even if the posting consists of hyperlinks, is still covered here by CA 2003 as held in relevant caselaw (*Chambers v DPP [2012] EWHC 2157; R (on the application of Alison Chabloz) v Crown Prosecution Service [2020] 1 Cr App R 17*). This is an important precedent, as social media accounts that generally post messages with gen-AI CSAM can be held accountable here.

As for the offender's *mens* rea, in *DPP v Kingsley Smith [2017] EWHC 359 (Admin)*, it was admitted that the offender "intended his message be grossly offensive to those to whom it related; or that he was aware at the time of sending that it might be taken to be so by a reasonable member of the public who read or saw it".

CA 2003 extends the criminal liability to corporate bodies and company directors. In s404, the law states that:

> *"(1)Where an offence under any enactment to which this section applies is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of—*
>
> *(a)a director, manager, secretary or other similar officer of the body corporate, or*
>
> *(b)a person who was purporting to act in any such capacity,*
>
> *he (as well as the body corporate) is guilty of that offence and shall be liable to be proceeded against and punished accordingly.*
>
> *(2)Where an offence under any enactment to which this section applies—*
>
> *(a)is committed by a Scottish firm, and*
>
> *(b)is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of a partner of the firm,*
>
> *he (as well as the firm) is guilty of that offence and shall be liable to be proceeded against and punished accordingly.*
>
> *(3)In this section "director", in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate."*

The most recent legislative development with regards to online child protection and safeguarding in the UK is undoubtedly the UK's *Online Safety Act 2023* (*OSA 2023*). This Act increased regulatory powers to OFCOM with regards to communications networks and services across the country. Prior to the *OSA 2023*, OFCOM's regulatory authority covered on-demand programme service (s368B CA 2003) and video-sharing platform service providers (s368T CA 2003). Now, with *OSA 2023* having been introduced, OFCOM's reach extends to services such as user-to-user services, meaning any "internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by [...] other users of the service"; and search services, meaning search engines, as per s3(1) and s3(4). S236 of the *OSA 2023* defines content as "anything communicated by means of an internet service", publicly or privately which may include among other things "photographs, videos, visual images [...] and data of any description". As opposed to *CA 2003*, which extended OFCOM's regulatory powers to services that have a mostly territorial link with the UK (see s368A and 368S), the *OSA 2003* extends OFCOM's powers to services even if they do not have territorial links with the UK, but instead simply have users in the UK; the UK is a targeted market; and as such there can be harm to UK users arising from this service (see s4).

Under *OSA 2023*, respective service providers now have the duty to "identify, mitigate and manage the risks of harm" from "content and activity that is harmful to children" as per s1(2)(a)(ii) by creating platforms that are "safe by design" and which afford "a higher standard of protection [...] for children than for adults", whilst still protecting "users' rights to freedom of expression and privacy", as per s1(3). Simultaneously, the Secretary of State is tasked and empowered to take action on online child safety issues by setting strategic priorities (s172), provide guidance to OFCOM (s176) and review the operation of the regulatory framework provided for in the *OSA* (s178). Under this framework, carrying out risk assessments (see s9–11, 23, 28) and annual transparency reports to OFCOM (s77) are also duties imposed and aim towards illegal content prevention, including CSAM.

CA 2003, in s368E(2), states that on-demand programme services "must not contain any prohibited material", defined as "material the inclusion of which in an on-demand programme service would be conduct required" to be an offence by Article 5(4) of *EU Directive 2011/93* [s368E(3)(za) and s368E(3)(za)(ii)]. Therefore, this leaves it unclear as to whether the detection and removal of computer-generated CSAM that may involve a real or imaginary child is included under the concept of "prohibited material". The non-binding Interim Code of Practice does instruct companies that operate online platforms to identify and remove CSAM that takes the form of "pseudo images" – photos, images, and videos "made, for example, on a computer, but which look like real photographs" and which "can include photos, videos, tracings and derivatives of a photograph and data that can be converted into a photograph" (Home Office, 2020: 7, 9).

On the other hand, the *OSA* is clearer on the matter of artificial CSAM, containing provisions that indicate the inclusion of artificial CSAM within its regulatory scope and therefore within the preventative and detecting scope of service providers. S55(4) states that regulated user-generated content includes "content generated, uploaded or shared by means of software or an automated tool applied by the user". Then, s59(3) defines "illegal content" as "content consisting of certain words, images, speech or sounds amounts to a relevant offence" in the following three cases: "if (a)the use of the words, images, speech or sounds amounts to a relevant offence;(b) the possession, viewing or accessing of the content constitutes a relevant offence, or (c)the publication or dissemination of the content constitutes a relevant offence". Further, s59(9) defines "CSEA content" as "content that amounts to an offence specified in Schedule 6" further labelling it as "priority illegal content" [s59(10)]. The same section adds that references to illegal content in the Act "are not to be taken to prevent content generated by a bot or other automated tool from being capable of amounting to an offence", thus opening the interpretation of CSEA content to include content created by AI. Examining Schedule 6 of the *OSA*, we can conclude that CSAM becomes "priority content" in the eyes of the law and is defined with reference to all key pieces of legislation detailed above and which revolve around the regulation of indecent photographs/pseudo-photographs, images/pseudo-images and paedophile manuals. Thus, the *OSA* serves as the gluing element that links all relevant legislation together, essentially regulating the phenomena mentioned in various pieces of legislation around the possession and dissemination of CSAM/pseudo-CSAM in the backdrop of user-to-user and search services. And as such, it provides adequate coverage in terms of gen-AI CSAM that may be disseminated in the regulated services, with the drawbacks mentioned above regarding the gaps that the primary legislation (which the *OSA* cites in Schedule 6) has.

"Where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way", then the provider must "swiftly take down such content", as per to s10(3)(b). This action is defined in s236(1) as "any action that results in content being removed from a user-to-user service or being permanently hidden so users of the service cannot encounter it". As per s10(2)(b), illegal content safety duties include preventative measures too.

Regulated services under the *OSA 2023* can use proactive technology to comply with illegal content and children's safety duties (see s10, 12, 27 and 29). This includes content identification technology "such as algorithms, keyword matching, image matching or image classification, which analyses content to assess whether it is content of a particular kind (for example, illegal content)", as per s231(2). According to s121(1), "If OFCOM consider that it is necessary and proportionate to do so, they may give a notice [...] to the provider of the service", which may require the provider to use accredited technology or develop new technology in order to identity and swiftly take down CSAM content on the platform that is communicated publicly or privately and swiftly take it down, as per s121(2)-(3).

Criminal Liability for Omission: Duties to Protect from AI-Generated CSAM

English criminal law generally imposes no criminal liability for “commission by an omission”. This means that an individual cannot typically be held criminally liable for failing to act unless they have a positive legal duty to do so. Criminal liability for failing to act only arises when the defendant has a specific legal duty to prevent harm or intervene in a dangerous situation. More specifically, such duties may arise from:

a) a close personal relationship

b) assumed responsibilities when a person voluntarily assumes responsibility for another’s care

c) when an individual creates a dangerous situation and then fails to act to prevent harm (*R v Miller [1983] 2 AC 161* and *R v Evans [2009] 2 Cr App R*)

d) other legal and contractual duties (*R v Pittwood [1902] TLR 37*).

Today’s challenges with the fast growth of AI may indicate a need for such duties of care to evolve and encompass safeguarding children from AI-generated material. While the law has yet to address cases involving AI-generated CSAM, there may be some instances where criminal liability for omissions could logically extend to these scenarios. These are the cases of close personal relationship, i.e. cases of parents who have a duty of care to protect their children from harm (in this case harm related to AI-generated CSAM) and failed to take appropriate action. Or the case of assumed responsibilities, i.e.

guardians and carers of children who failed to take appropriate actions to protect their children from all types of harm related to AI-generated CSAM.

Civil law responsibility for AI-generated CSAM under the *Data Protection Act 2018*

Currently, there is no specific legislation or case law in the UK that directly addresses this issue from a civil law perspective. This leaves a significant gap in how the law handles such new emerging threats. However, AI-generated CSAM could potentially fall under the protections offered through the *Data Protection Act 2018*.

The *Data Protection Act 2018* applies to the entire UK, implementing the EU's *General Data Protection Regulation* (*GDPR*). This legislation covers personal data following *GDPR* (s.1). For this discussion, it is interesting that it extends to information relating to an identifiable person, such as images of digital likenesses, presumably even if AI-generated (s.8).

More specifically, section 2 of the *Data Protection Act 2018 Act* protects individuals from the processing of personal data, in particular through:

> *"a) requiring personal data to be processed lawfully and fairly, based on the data subject's consent or another specified basis,*
>
> *b) conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and*
>
> *c)conferring functions on the Commissioner, giving the holder of that office responsibility for monitoring and enforcing their provisions."*

The term "processing" is defined in s3(4) as:

> “an operation or set of operations which is performed on information, or sets of information, such as
>
> *a) collection, recording, organisation, structuring or storage,*
>
> *b) adaptation or alteration,*
>
> *c) retrieval, consultation or use,*
>
> *d)disclosure by transmission, dissemination, or otherwise making available,*
>
> *e) alignment or combination, or*
>
> *f) restriction, erasure or destruction”*

Thus, it seems that under the legislation, if a child's identifiable image or likeness is used without permission, it falls under the scope of section 2 and the definition of “processing” personal data. This interpretation of the legislation suggests that entities involved in creating or distributing AI-generated CSAM could be liable for unlawful processing under the legislation. Creating or distributing AI-generated CSAM conflicts with the principle of lawful processing, which requires consent or at least another specified, lawful basis, defined in s8.

The *2018 Act* further imposes obligations on platforms or services enabling or hosting AI-generated content to integrate safeguards that prevent the misuse of personal data. In particular, section 57 emphasises the need for data protection “by design and default”. This is important as it requires controllers to implement technical and organisational measures to safeguard personal data during processing. The legislation details the responsibilities of processors to act strictly on controllers' instructions and maintain confidentiality (ss. 59 and 60, *Data Protection Act 2018*). Failure to uphold these principles exposes platforms to liability, which requires data protection impact assessments and cooperation with the Commissioner to mitigate risks to individuals' rights and freedoms (ss. 64 and 63, *Data Protection Act 2018*).

This legislative framework aims to prevent and address misuse. This could logically extend to cases of AI-generated CSAM, even though this is not specifically mentioned in the Act's provisions. Nonetheless, there is a clear emphasis on the platforms' duty to proactively prevent breaches and uphold compliance (*Data Protection Act 2018*). In this sense, the Act seems to obligate platforms or services enabling or hosting AI-generated content to build safeguards avoiding the misuse of personal data. Failure to do so may expose these platforms to liability for not complying with data protection principles, especially if they enable or fail to prevent CSAM.

Under section 168 of the *Data Protection Act 2018*, individuals may seek compensation for damage caused by a data breach or misuse. Thus, if a child's likeness is used without authorisation in explicit AI-generated content, they or their guardians can claim damages for emotional and psychological harm. The legislation extends those compensation rights under the *UK GDPR* to "non-material damage", such as distress caused by a contravention of the regulation. This explicit recognition is significant since it reinforces the legislation's commitment to addressing emotional harm, providing victims of AI-generated CSAM with a possible legal route. If a representative body initiates proceedings for compensation on behalf of an individual, and the court orders compensation, the court may direct the payment to either the representative body or another party if deemed appropriate (*Data Protection Act 2018*).

In conclusion, the existing framework under the *Data Protection Act 2018* provides a good foundation for tackling this emerging issue. However, as AI technologies continue to advance, addressing these complex issues may require more targeted legislative reforms in addition to the existing legislation to ensure adequate protection for children.

Compensation

There are various ways in which victims of crimes can claim compensation in the UK. However, their applicability is put under question with regards to CSAM created via gen-AI technologies. Also, their applicability (if any) is best suited for gen-AI CSAM that includes childlike figures modelled after real children rather than CSAM that includes artificial children. This is because in the latter case, there is no identifiable victim that has sustained physical or psychological harm who can then be eligible for a civil claim.

In England and Wales, criminal courts can give an offender a compensation order after the said offender is convicted. Another pathway to compensation would be via the Criminal Injuries Compensation Scheme addressed to the Criminal Injuries Compensation Authority (CICA). To be eligible for this pathway, the crime must be reported to the police and the claim must be made by their 20th birthday, if the victim was under 18 at the time of the incident (although the time limit can be extended in exceptional circumstances and after evidence justifying why the claim could not be made before is submitted and accepted); and have no criminal record. The positive aspect of the CICA pathway is that it is a good compensation option if the offender does not possess the funds to compensate the victim. However, the main issues with this option is first that CICA is tied to the victim's UK residency at the time of the incident, combined with nationality requirements: the victim needs to be either British, or close relative of a British citizen, or citizen of EU/EEA, or a national of a State party to the Council of Europe Convention on the Compensation of Victims of Violent Crimes, or asylum seeker or trafficking victim. Adding to that is the incident location requirement, according to which the crime location can only be England, Scotland, Wales or another "relevant place" (royal vessel, hovercraft etc.). The way this guidance is phrased indicates that CICA seems more tailored and more comfortably applied for in-person offline crimes that are tied to UK territory and occur against people of certain citizenships or immigration statuses. Therefore, CICA's applicability on online crimes is more challenging, but is still deemed possible, respecting the rules set by this Scheme and which revolve around the citizenship and location of the victim at the time of the incident.

The other frequently used route for compensation, especially given CICA's time, citizenship, location and award limitations, is via a civil claim, usually for personal injury due to psychological harm endured, given that grounds for compensation on the basis of physical injury are unlikely in the studied case. Another legal basis for compensation would be via a claim for privacy infringements based on the *UK GDPR* for misuse of private information and/or breach. Damages can thus be recovered for the infringement itself, as well as for any feelings of distress, anxiety and embarrassment caused as a consequence of the said infringement/breach.

Nonetheless, the main issue around the applicability of UK civil law legislation on CSAM created via AI revolves around the question who is considered the author of the gen-AI material. This would subsequently define who is responsible party for any gen-AI produced work. In the UK, the person who is considered the author of a computer-generated work is the one who makes the arrangements necessary for the work to be created. According to s9(3) of the *Copyright Designs and Patents Act 1988*, this shall be "taken to be the person by whom the arrangements necessary for the creation of the work are undertaken". Therefore, the UK's wide and encompassing phrasing in this case seems to be fitting the cases of computer-generated work, at least in principle. Still, the applicability of this section remains unclear, as it refers to "literary, dramatic, musical or artistic work". Caselaw interpretation in future cases going through this pathway will be therefore crucial to define applicability. Also, it remains to be clarified whether in the case of gen-AI CSAM (but also in the case of other non-indecent material created via gen-AI), this would mean the individuals involved in writing the code based on which the AI operates; those who trained the AI software; or those who operate and use the software. Therefore, the liability for any AI-produced works, including indecent products, such as CSAM remains currently unclear under existing legislation across the UK. This calls for either an updating of existing legislation; or introduction of new legislation; or lastly, in the case that policymakers wish to avoid the phenomenon of overregulation, this calls for a wide interpretative work by courts to fit cases of AI-generated material under existing legislation.

Legal Reforms

Regarding legal reforms, as seen above, there are upcoming updates on deepfake pornography for adults and paedophile manuals. Another recent legal reform concerns AI tools. More specifically, the UK is planning to make it illegal to possess, create or distribute AI tools designed to create CSAM, with a punishment of up to five years in prison (Home Office, 2025; see section 63 Crime and Policing Bill on CSA Image Generators).

As for the UK *OSA*, there is ongoing discussion around potential updates which revolve predominantly around stricter rules against hate speech online (Coulter, 2024). On this, reforming OSA with regards to online child protection seems to be a secondary priority, with mostly informal discussions around it. It is not yet clear what these potential reforms may entail.

As regards targeted AI legislation in the form of an AI Act, the EU has recently introduced its own *Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024*, which lays down harmonised rules on AI. As stated in the Regulation, "aside from the many beneficial uses of AI, it can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices", which are "particularly harmful and abusive and should be prohibited because they contradict Union values of respect for [...] the rights of the child". As further explained, "the extent of the adverse impact caused by the AI system on fundamental rights [...] is of particular relevance when classifying an AI system as high risk". Among these fundamental rights, the rights of children are also being specifically mentioned and prioritised. This new industry regulation for AI in the EU categorises AI systems/models based on their risk under 4 categories: unacceptable, high, limited and minimal risk. Other countries are already subscribing to the notion of AI regulation through legislation, such as Brasil.

Despite rumours around a UK *AI Act* with a new Labour administration and following the result of the 2024 general election in the UK, the King's speech did not mention a standalone UK AI Act within the paradigm of upcoming new laws and legislative updates. Therefore, the most likely form these AI-related updates might take in the UK for the time being would be targeted legislative updates and additions within existing acts rather than a standalone UK AI Act.

Conclusion and Recommendations

In conclusion, legislation across the UK is phrased in a broad and tech agnostic way, rendering it applicable to gen-AI CSAM. The role that is assigned to courts across the UK, which have significant leeway to interpret legislation on a case-by-case basis increases this applicability of existing laws to AI-generated CSAM.

That said, there are some gaps in legislation, which could be addressed, and in fact some of them are being addressed currently through ongoing legislative updates. These gaps were more evident in Scotland rather than the rest of the UK. They revolve around topics such as non-photographic indecent imagery of children (gap in the criminalisation of the act of making for England and Wales; no relevant legislation found on non-photographic indecent imagery of children in Scotland); paedophile manuals (gap in the criminalisation of producing a paedophile manual to create pseudo-CSAM; no relevant legislation that criminalises paedophile manuals found in Scotland). On top of that, the use of a heavily gendered language (frequent use of the pronoun "he" for offenders) may restrict the scope of criminal justice efforts.

Despite the absence of case law on criminal liability for omissions in cases of AI-generated CSAM, the argument that it is possible that such liability may arise under the categories of close personal relationships and assumed responsibilities (parents and guardians) might have theoretical basis.

From a civil perspective, there is no specific legislation or case law in the UK that directly addresses this issue. However, AI-generated CSAM does seem to fall under the protections offered through the *Data Protection Act 2018*.

Generally, the applicability of the various ways in which victims of crimes can claim compensation in the UK extends to cases of gen-AI CSAM. However, the applicability of compensation schemes such as CICA are put under question. As expected, compensation concerns the case where childlike figures are modelled after real children, since in the case that the child is purely fictitious, no identifiable victims exist.

The main practical, but also theoretical recommendations arising from the abovementioned legislative analysis are the following:

Recommendation 1. Update the law to clearly criminalise all acts relevant to pseudo-photographs that depict purely fictitious children, i.e., making, taking, disseminating and possessing such material.

Recommendation 2. The Scottish Government should introduce legislation to criminalise all acts relevant to non-photographic indecent images of children, i.e., making, taking, disseminating and possessing such material.

Recommendation 3. Amend existing legislation that is in force in England and Wales to criminalise the making of indecent non-photographic imagery of children

Recommendation 4. Update UK legislation on paedophile manuals to make it applicable on pseudo-photographs; and on criminal responsibility for software creators. As stated above, reforms on the matter are currently underway.

Recommendation 5. Strengthen legislative protection against all forms of paedophile manuals in Scotland.

Recommendation 6: Amend language used in UK-wide legislation to make it more inclusive, wide and encompassing

References

Literature Review and Methodology

Bahoo, S., Cucculelli, M., & Qamar, D. (2023). Artificial intelligence and corporate innovation: A review and research agenda. *Technological Forecasting & Social Change*, 188. https://doi.org/10.1016/j.techfore.2022.122264

Fisher, C., Goldsmith, A., Hurcombe, R., & Soares, C. (2017). *The impacts of child sexual abuse: A rapid evidence assessment*. Independent Inquiry Into Child Sexual Abuse. Retrieved from https://www.iicsa.org.uk/reports-recommendations/publications/research/impacts-csa.html

Huang, J, C. (2022). From Building Information Modeling to Extended Reality. In M. Bolpagni, R. Gavina & D. Ribeiro (Eds.), *Industry 4.0 for the Built Environment Methodologies: Technologies and Skills* (pp. 471-494). New York: Springer.

Internet Watch Foundation. (2023). *How AI is being abused to create child sexual abuse imagery*. Retrieved from https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

Lee, H., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*, 34, 1-11. https://doi.org/10.1016/j.fsidi.2020.301022

McConville, M., & Chui, W.H. (2007). Introduction and overview. In M. McConville & W.H. Chui (Eds.), *Research Methods for Law* (pp. 1-17). Edinburgh: Edinburgh University Press.

Ness, S., Riley, C., & Bantourakis, M. (2023, September 23). Digital Governance over online safety is at risk of fragmenting. A multistakeholder approach could prevent that. World Economic Forum. Retrieved from https://www.weforum.org/stories/2023/09/its-time-for-global-alignment-on-digital-governance/

Ngo, N. (2021). Child sexual abuse violence against human dignity of children. *International Journal of Research Studies in Education*, 10(15), 97-108. https://doi.org/10.5861/ijrse.2021.a124

Ngo, N., McKeever, S., & Thorpe, C. (2023). *Determining Child Sexual Abuse Posts based on Artificial Intelligence*. Technological University Dublin. Retrieved from https://arrow.tudublin.ie/scschcomcon/392/

Parti, K., & Szabo, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws*, 13(6), 67. https://doi.org/10.3390/laws13060067

Quayle, E. (2016). *METHOD GUIDE 7: Researching online child sexual exploitation and abuse: Are there links between online and offline vulnerabilities?* Global Kids Online. Retrieved from http://globalkidsonline.net/wp-content/uploads/2016/05/Guide-7-Child-sexual-exploitation-and-abuse-Quayle.pdf

Simon, J., Luetzow, A., & Conte, J.R. (2020). Thirty years of the convention on the rights of the child: Developments in child sexual abuse and exploitation. *Child Abuse & Neglect*, 110, 1-8. https://doi.org/10.1016/j.chiabu.2020.104399

Weaver, J.M., & Røseth, T. (2024). The "Five Eyes" Intelligence Sharing Relationship : A Contemporary Perspective (1st ed. 2024.). London: Springer International Publishing.

Wright, L. (2018). Black-Letter Law. *LawNow Magazine*. https://www.lawnow.org/black-letter-law/

United Kingdom

Abusive Behaviour and Sexual Harm (Scotland) Act 2016 (Scotland)

Anderson [1972] 1 QB 304

Anti-social Behaviour, Crime and Policing Act 2014 (UK)

Atkins v Director Of Public Prosecutions | [2000] 2 All ER 425

Chambers v DPP [2012] EWHC 2157

Civic Government (Scotland) Act 1982 (Scotland)

Communications Act 2003 (UK)

Connolly v DPP [2007] 2 ALL ER 1012

Copyright Designs and Patents Act 1988 (UK)

Coroners and Justice Act 2009 (UK)

Coulter, M. (2024). *UK revisits social media regulation after far-right riots*. Reuters. https://www.reuters.com/world/uk/uk-revisits-online-safety-act-after-far-right-riots-2024-08-

09/#:~:text=The%20act%2C%20passed%20in%20October,to%20violence%20or%20hate%20speech.

Crime and Policing Bill (UK)

Criminal Justice (Evidence, etc.) (Northern Ireland) Order 1988 (NI)

Crown Prosecution Service. (2019). *Obscene Publications*. https://www.cps.gov.uk/legal-guidance/obscene-publications

Crown Prosecution Service. (2022). *Sex Dolls – Childlike*. https://www.cps.gov.uk/legal-guidance/sex-dolls-childlike

Crown Prosecution Service. (2024a). *Indecent and Prohibited Images of Children*. https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children

Crown Prosecution Service. (2024b). *Communications Offences*. https://www.cps.gov.uk/legal-guidance/communications-offences

Customs and Excise Management Act 1979 (UK)

Customs Consolidation Act 1876 (UK)

Data Protection Act 2018 (UK)

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

DPP v Bussetti [2021] EWHC 2140 (Admin)

DPP v Collins [2006] 1 WLR 2223

DPP v Collins [2006] UKHL 40

DPP v Kingsley Smith [2017] EWHC 359 (Admin)

Gawne, E. (2024). *Man who made 'depraved' child images with AI jailed*. https://www.bbc.co.uk/news/articles/cq6l241z5mjo

General Data Protection Regulation (EU)

Goodland v DPP [2000] 2 Cr. App. R. 248

Home Office. (2020). *Interim Code of Practice on Online Child Sexual Exploitation and Abuse*. UK Government, Home Office. https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-online-child-sexual-exploitation-and-abuse-accessible-version

Home Office. (2025). Britain's leading the way protecting children from online predators. UK Government, Home Office. https://www.gov.uk/government/news/britains-leading-the-way-protecting-children-from-online-predators#:~:text=make%20it%20illegal%20to%20possess,to%203%20years%20in%20prison

Internet Watch Foundation. (2024). *IWF response to the Science, Innovation, and Technology Committee Inquiry: Governance of Artificial Intelligence (AI).*

Interpretation Act (Northern Ireland) 1954 (NI)

Justice (Sexual Offences and Trafficking Victims) Act (Northern Ireland) 2022 (NI)

Justice Act (Northern Ireland) 2016 (NI)

Malicious Communications Act 1988 (UK)

Obscene Publications Act 1959 (UK)

Office of Communications Act 2002 (UK)

Online Safety Act 2023 (UK)

Police, Crime, Sentencing and Courts Act 2022 (UK)

Policing and Crime Act 2017 (UK)

Postal Services Act 2000 (UK)

Protection of Children (Northern Ireland) Order 1978 (NI)

Protection of Children Act 1978 (UK)

R (on the application of Alison Chabloz) v Crown Prosecution Service [2020] 1 Cr App R 17

R v DM [2011] EWCA Crim 2752

R v Dooley [2006] 1 Cr. App. R. 21

R v Evans [2009] 2 Cr App R

R v Graham-Kerr (1989) 88 Cr. App. R. 302

R v Harrison [2008] 1 Cr. App. R. 29

R v Jayson [2003] 1 Cr. App. R. 13

R v Miller [1983] 2 AC 161

R v Neal [2011] EWCA Crim 461

R v Owen (1988) 86 Cr. App. R. 291

R v Penguin Books Ltd

R v Pittwood [1902] TLR 37

R v Smethurst [2002] 1 Cr. App. R. 6

R v Smith and Others [2011] EWCA Crim 1772

R v Smith (Thomas Joseph) [1959] 2 QB 35

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Ryan-White, G. (2022*). Cyberflashing and Deepfake Pornography*. Northern Ireland Assembly. https://www.niassembly.gov.uk/globalassets/documents/raise/publications/2017-2022/2022/justice/0122.pdf

Serious Crime Act 2015 (UK)

Sexual Offences (Northern Ireland) Order 2008 (NI)

Sexual Offences Act 2003 (Notification Requirements) (England & Wales) Regulations 2012 (England and Wales)

Sexual Offences Act 2003 (UK)

Whyte [1972] 3 All ER 12

More information

Suggested citation: Gaitis, K.K., Fakonti, C., Lu, M., Stevenson, J., & Fry, D. (2025). Legal challenges in tackling AI-generated child sexual abuse material across the 5 Eyes nations: Who is accountable according to the law? United Kingdom. Edinburgh: Childlight – Global Child Safety Institute

Registered study protocol: OSF Registries | Does existing legislation on CSEA/CSAM across the Five Eyes nations and India allow for criminal liability or any other form of accountability with regards to AI-generated CSAM?

Ethics approval: University of Edinburgh, Childlight Research Ethics Sub-Committee (DELOC-KKG-0030424CL)

Advisory committee members: Professor Ben Mathews (School of Law, Queensland University of Technology), Dan Sexton (Chief Technology Officer, Internet Watch Foundation), Michael Skwarek (Manager, Codes and Standards Class 1, Industry Compliance and Enforcement, Australian eSafety Commissioner)

Funding acknowledgement: The research leading to these results has received funding from the Human Dignity Foundation under the core grant provided to Childlight – Global Child Safety Institute under the grant agreement number [INT21-01].