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 STATES OF AMERICA

Authors:

Ms Jessica Schidlow
Legal Director, Child USA

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

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

AB – Assembly Bill

AI – Artificial Intelligence

AK – Alaska

AL – Alabama

AR – Arkansas

AZ – Arizona

C.F.R. – Code of Federal Regulations

CA – California

CDA – Communications Decency Act

CODE ANN. – Code Annotated

COMP. STAT. – Compiled Statutes

COPPA 2.0 – Children and Teens' Online Privacy Protection Act

CPPA – Child Pornography Prevention Act

CSAM – Child Sexual Abuse Material

DE – Delaware

DEFIANCE – Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024

DMCA – Digital Millennium Copyright Act

EARN IT Act – Eliminating Abusive and Rampant Neglect of Interactive Technologies

ELVIS Act – Ensuring Likeness, Voice, and Image Security Act of 2024

FL – Florida

FOSTA-SESTA – Fight Online Trafficking Act and the Stop Enabling Sex Traffickers Act

FTC – Federal Trade Commission

GA – Georgia

GEN. LAWS – General Laws

HB – House Bill

HI – Hawaii

IA – Iowa

ICMEC – International Centre for Missing & Exploited Children

ID – Idaho

IL – Illinois

IN – Indiana

KAN – Kansas

KOSA – Kids Online Safety Act

KY – Kentucky

LA – Louisiana

MA – Massachusetts

MD – Maryland

ME – Maine

MI – Michigan

MINN – Minnesota

MO – Missouri

MT – Montana

NC – North Carolina

NCII – Non-Consensual Intimate Imagery

NCMEC – National Center for Missing and Exploited Children

ND – North Dakota

NE – Nebraska

NIST – National Institute of Standards and Technology

NJ – New Jersey

NM – New Mexico

NMI – Northern Mariana Islands

NO AI FRAUD – No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act

NO FAKES – Nurture Originals, Foster Art, and Keep Entertainment Safe Act

NV – Nevada

NY – New York

OECD – Organisation for Economic Co-operation and Development

OK – Oklahoma

ON – Ontario

OR – Oregon

PA – Pennsylvania

PROTECT Act (2003) – Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act

PROTECT Act (2008) – Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act

RC – Refused Classification

REPORT Act – Revising Existing Procedures on Reporting via Technology Act

REV. STAT. – Revised Statutes

RI – Rhode Island

SB – Senate Bill

SD – South Dakota

STAT. – Statutes

STOP CSAM Act – Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act

TX – Texas

U.S.C. – United States Code

USA – United States of America

USCO – U.S. Copyright Office

UT – Utah

V.I. – U.S. Virgin Islands

VA – Virginia

VAWA – Violence Against Women Act Reauthorization Act of 2022

WA – Washington

WI – Wisconsin

WV – West Virginia

WY – Wyoming

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 USA; 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, as well as their progressive legislative systems.

In the United States of America (USA), the regulatory framework consists of federal laws and state-based laws. Federal CSAM statutes, together with case law, criminalise several categories of harmful material. Still, a significant number of vague points persist. Federal laws are relatively robust, but there is a gap with regards to the criminalisation of artificial CSAM that depicts purely fictitious children. Civil remedies, although significant, are limited in scope. Copyright and consumer protection laws offer some avenues for redress, but they are also limited. Prosecutors typically require concrete evidence to prosecute, such as incriminating communication or attempts to sell or trade material. These are often hard to obtain. This challenge is increased by more advanced AI models that generate hyper-realistic CSAM without training on authentic abuse imagery. This means that even if we start regulating how AI models are trained, these advanced AI models that can create realistic CSAM without the need for training will be evading regulation.

Drawing on copyright law, platforms and developers can be held liable if they knowingly contribute to the sharing of harmful content. However, online

platforms are protected from civil liability for user-generated content, complicating efforts to hold them accountable for hosting AI-generated CSAM. Despite efforts to change the law on this, balancing platform liability with the protection of free speech is a major challenge.

The legal landscape is even more fragmented on a state level due to several outdated pieces of legislation around so-called “child pornography”[1], which fail to address newer forms of technology-facilitated child sexual abuse (TF-CSEA). State-level civil remedies are often inadequate, leaving gaps in accountability for users, developers, distributors and third-party beneficiaries.

On 16 April 2024, the H.R.8005 - Child Exploitation and Artificial Intelligence Expert Commission Act of 2024 was introduced to address the creation of child sexual abuse material (CSAM) using artificial intelligence (AI). This legislation would establish a commission to develop a legal framework that would assist law enforcement in preventing, detecting, and prosecuting AI-generated crimes against children. Based on these findings, the following recommendations are made for the USA:

Recommendation 1. Amend existing CSAM laws to explicitly cover AI-generated content, even when it includes fictitious children.

Recommendation 2. Amend CSAM laws to regulate the misuse of AI.

Recommendation 3. Establish a legally binding framework for safe and responsible AI development and deployment.

Recommendation 4. Expand legal protections to include control over one’s own image.

[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.

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 primarily 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, and 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 process than socio-legal analyses, which tend to look 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 were eligible for inclusion, if they focused on any area intersecting with accountability for CSEA/CSAM particularly with regard to generative AI software. They were also included if they defined concepts applicable to AI-generated CSAM, such as 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 five countries, we conducted an initial search of legal websites, such as Lexis Nexis, Practical Law, Google Scholar and Google; utilised official Government sources; and searched on local court and prosecution services' websites.

Regarding US, platforms such as National Conference of State Legislatures, Multistate AI Legislation Tracker and Legiscan were additionally used to retrieve legal sources.

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, we consulted with our extensive network of experienced colleagues located in these countries. They assisted us in locating further legislation 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 the 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", "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:

- 56- U.S. state and territory CSAM criminal laws
- 22- U.S. state and territory CSAM civil laws
- 20- U.S. state cases re: criminal CSAM laws
- 5- U.S. federal CSAM/obscenity related laws

- 27- U.S. federal cases re: CSAM
- 56- U.S. state and territory obscenity (criminal) laws
- 56- U.S. state image-based abuse laws (i.e. revenge porn, deepfakes)
- 1-U.S. federal image-based abuse law
- 33- U.S. pending state legislation re: AI governance
- 17- U.S. pending federal legislation re: AI governance/AI accountability
- 52- U.S. state privacy tort laws (statutory and common law)
- 3- U.S. Misc. federal laws

Legislative Review: USA

“Child Pornography” and “Obscenity” Laws

The framework for regulating CSAM in the United States reflects a delicate balance between the government’s compelling interest in protecting children from abuse and exploitation and the First Amendment’s free speech protections *(U.S. CONST. amend. 1)*.[2] Two landmark Supreme Court cases, *Miller v. California (1973)* and *New York v. Ferber (1982)*, have significantly shaped this framework,[3] affirming that CSAM is categorically excluded from First Amendment protection. These decisions grant federal and state governments broad authority to regulate the possession, production, and distribution of such materials. That said, the *Ferber* case’s ruling focused on content that directly harms real children, leaving other indirect harms and the case of imaginary children out of its regulatory scope. Congress attempted to close this loophole with its *Child Pornography Prevention Act (CPPA),* which expanded the definition of “child pornography” to include virtual or computer-generated images (CGI) that “appear to” depict or “convey the impression” of minors engaging in sexually explicit conduct *(CPPA, 1996)*. However, in *Ashcroft v. Free Speech Coalition*, the Supreme Court struck down these portions of the CPPA as overly broad. In other words, images that contain adults with childlike features or CGI representations were found to be outside the regulatory scope of *Ferber.* Therefore, the *Ashcroft* decision has created a gap with regards to regulating and banning AI-generated CSAM which does not include a real, but instead an imaginary child.

[2] The First Amendment states, "Congress shall make no law ... abridging the freedom of speech." U.S. CONST. AM. 1.

[3] *See also* Roth v. United States, 354 U.S. 476, 481 (1957) (“[T]his Court has always assumed that obscenity is not protected by the freedoms of speech and press”).

In response to *Ashcroft*, Congress enacted the *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (PROTECT Act),* to broaden the definition of "child pornography" to include digital and computer-generated representations of children "indistinguishable" from real children. The Act also prohibited the acts of advertisement, promotion, presentation, or distribution of CSAM, including material that does not constitute "child pornography", but is promoted as such *(PROTECT Act, s.151)*. In *United States v. Williams*, the Supreme Court upheld the constitutionality of this provision, but at the same time confirmed that virtual CSAM "do[es] not involve, let alone harm, any children in the production process", is "not intrinsically related to the sexual abuse of children" and thus "records no crime[,] and creates no victims by its production."

The Federal Statutory Framework

The federal framework for addressing AI-generated CSAM relies primarily on two statutes codified in Title 18 of the U.S. Code (1996): 18 U.S.C. §2252A, which prohibits the possession, production, receipt, and distribution of "child pornography" and 18 U.S.C. §1466A, which prohibits the production, receipt, and possession of obscene visual depictions involving minors.

For purposes of § 2252A, "child pornography" is defined as any "visual depiction" of sexually explicit conduct involving a minor, including CGI. However, the law emphasises that it applies to depictions of an "identifiable minor" (18 U.S.C. § 2256). This entails that the law covers AI-generated CSAM, but only if real, identifiable minors are included in this material. The challenge for prosecution therefore increases with the advent of second-generation AI models that generate hyper-realistic CSAM without training on authentic abuse imagery, effectively evading regulation under statutes like 18 U.S.C. § 2256, which narrowly defines CSAM as involving identifiable minors. As for 18 U.S.C. §1466A, this also includes CGI and additionally explicitly states that it does not require "that the minor depicted exist." *(§§ 1466A(c), 1466(f)(1))*.

Violations of § 2252A can result in severe penalties of imprisonment, while 18 U.S.C. §2259 requires defendants convicted under §2252A(9), relating to trafficking in CSAM, to pay restitution to victims.

Federal law also enables "[a]ny person aggrieved" by a CSAM crime, including an offense under §2252A or §1466A, to initiate a civil action for temporary, preliminary, or permanent injunctive relief and to seek compensatory and punitive damages as well as attorneys' fees (*§2252A(f)(1)-(2))*. Victims who suffer "personal injury" due to a defendant's violation of § 2252A may also seek redress under 18 U.S.C. § 2255, also known as Masha's Law,[4] against those who initially produced the abusive material but also those who distribute it.

The State Statutory Framework

Offenders can also be prosecuted under state "child pornography" and "obscenity" laws in addition to, or instead of, federal law (U.S. Department of Justice, 2020). Consequently, at least 39 states and 1 U.S. territory have "child pornography" statutes broad enough to potentially cover AI-generated CSAM.[5] Of those states, 15 explicitly prohibit morphed images and synthetic CSAM,

[4] Importantly, § 1466A is not one of the predicate offenses covered under Masha's Law.

[5] These jurisdictions are Alabama, Alaska, Arizona, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Kentucky, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin, Wyoming, Northern Mariana Islands and the U.S. Virgin Islands.

provided the content is sufficiently realistic.[6] 14 states and 1 U.S. territory prohibit morphed images involving actual children, but do not extend to entirely synthetic, i.e. artificial content.[7] Meanwhile, 13 states and 4 U.S. territories do not appear to criminalise AI-generated CSAM at all.[8]

Even among states with statutes broad enough to potentially cover AI-generated CSAM, there is significant variability in their scope and outcome, depending on whether the state criminalises possession or only possession with intent to sell or distribute, often with the additional element of intent to sell for profit. Thirty states and 1 U.S. territory criminalise the distribution, dissemination, or publication of AI-generated CSAM.[9] At least 25 states and 1 U.S. territory prohibit the creation or production of AI-generated CSAM.[10] Some states, such as Alaska, Florida, and Texas, criminalise accessing or viewing AI-generated CSAM alone.

Most states with broadly written statutes explicitly reference “computer-generated images” or adopt broad and more generic terms like “any material” or “any representation” which serve to cover a range of abusive material. Some

[6] These states are Alabama, Alaska, Delaware, Florida, Idaho, Illinois, Kentucky, Michigan, Montana, Missouri, New Hampshire, North Carolina, South Dakota, Tennessee, and Virginia.

[7] These jurisdictions include Connecticut, Georgia, Hawaii, Maryland, Minnesota, Mississippi, Nebraska, New Jersey, Rhode Island, Texas, Utah, Washington, Wisconsin, Wyoming, and the US Virgin Islands. see Footnote 15.

[8] These jurisdictions are Colorado, Louisiana, Maine, Massachusetts, Nevada, New York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Vermont, West Virginia, Washington D.C., Guam, American Samoa, and Puerto Rico. see Footnote 15.

[9] The jurisdictions are Alabama, Alaska, Arizona, Arkansas, California, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kentucky, Maryland, Michigan, Montana, Mississippi, Minnesota, Nebraska, New Jersey, New Mexico, North Carolina, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Virginia, Washington, Wisconsin, Wyoming and the U.S. Virgin Islands. *See* Footnote 15.

[10] The jurisdictions are Alabama, Alaska, Arizona, Arkansas, California, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Kentucky, Maryland, Missouri, Nebraska, New Hampshire, New Jersey, New Mexico, North Carolina, Rhode Island, South Carolina, South Dakota, Utah, Virginia, Wyoming, and the U.S. Virgin Islands.

states, including South Dakota, Tennessee, and Washington, specifically reference artificial intelligence in their statutes. Others, like Florida and Hawaii, have expanded the scope of their CSAM statutes to include fictional or digitally created content by adding language prohibiting "simulated" sexual conduct.

Beyond "child pornography" laws, all 50 states and 6 U.S. territories maintain obscenity statutes originally intending to protect minors from accessing sexually explicit materials. Many state laws use archaic definitions of obscene content and are thus unsuitable to address the risks and harms arising from modern digital technologies. Still, some states have updated their laws respectively. For example, California recently passed legislation that bans "obscene visual representations of the sexual abuse of children," including AI-generated images *(AB 1831, 2023-2024)*. Therefore, clear accountability for those using AI to create, distribute, or possess obscene material is established through this legislation.

In addition to criminal penalties, at least 21 states and 1 U.S. territory have enacted statutes that explicitly enable CSAM victims to pursue civil claims and seek damages for their injuries.[11] In states such as Florida, Connecticut, New Mexico, Louisiana, Texas, and Wisconsin, the government provides victims with compensation for mental health services such as counselling to address psychological trauma caused by the crime, irrespective of whether the offender was successfully prosecuted *(FL STAT. § 960.197; CONN. GEN. STAT. § 54-201 et. seq.; N.M. STAT. ANN. § 31-22-3 et seq; LA STAT. ANN. § 46:1802 et seq.; TEX. CODE CRIM. PRO. ANN. art. 56b.001 et. seq.; WI STAT. § 949.01 et seq)*. States such as Arizona, Idaho, Kentucky, New Jersey, Oregon, Pennsylvania, South Carolina, Tennessee, Utah, Vermont, Virginia, and West Virginia also have similar

[11] These jurisdictions include Alabama, Alaska, Florida, Kansas, Massachusetts, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Utah, Virginia, Washington, Wisconsin, and the Northern Mariana Islands..

programs to assist victims who have suffered emotional or physical harm due to a crime *(ARIZ. REV. STAT. ANN. § 41-2407; IDAHO CODE § 19-5304; KY. REV. STAT. ANN. § 421.500; N.J. STAT. ANN. § 52:4B-2; OR. REV. STAT. § 147.005; 18 PA. CONS. STAT. § 11.103; S.C. CODE ANN. § 16-3-1110; TENN. CODE ANN. § 29-13-104; UTAH CODE ANN. § 63M-7-502; VT. STAT. ANN. tit. 13, § 5451 et seq.; VA. CODE ANN. § 19.2-368.2; W. VA. CODE § 14-2A-1)*. In New Hampshire and Washington, these programs extend only to victims of crimes classified as felonies *(N.H. REV. STAT. ANN. § 21-M:8-h; WASH. REV. CODE § 7.68.020)*.

Regulatory Framework for Developers and Online Service Providers

To combat online child sexual exploitation, Congress passed the *Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008 (PROTECT Act),* which requires internet service providers in knowing possession of CSAM to make a timely report to the National Center for Missing and Exploited Children's (NCMEC) CyberTipline *(PROTECT Act, p.4229)*. Additionally, the *Revising Existing Procedures on Reporting via Technology (REPORT) Act* expands these reporting obligations *(REPORT Act, §§ 3, 4(a))*, mandating internet service providers to report "planned," "imminent," and "apparent" violations of federal CSAM laws occurring on their platforms. Additionally, the Act increases the statutory penalties failures to report online sexual exploitation of children. These obligations apply to violations under §2252A, not §1466A, i.e. to content that includes real children only.

On whether companies that develop or deploy gen-AI software can be held liable for illegal or harmful content that their software generates, we have to factor in the *Communications Act of 1934*, enacted as part of the *Communications Decency Act (CDA) of 1996. The Act* grants online service providers a limited defence from liability for third-party content hosted on their platforms *(47 U.S.C. § 230)*. §230(c)(1) protects providers and users of an "interactive computer service" from being treated as publishers of user-generated content, while §230(c)(2) grants immunity for good-faith efforts to restrict user access to offensive or indecent material.

The limited defence of §230's has been expanded in caselaw granting defence against liability not only for "publisher" claims but "distributor" claims as well *(e.g., Zeran v. Am. Online, Inc., 1997, pp. 331-333)*. Due to this broad interpretation, online service providers have evaded accountability for a variety of illicit activities on their platforms. Courts have limited immunity in cases where platforms act as "information content providers" by contributing "in whole or in part" to the creation or development of unlawful content *(e.g., FTC v. Accusearch Inc., et al, 2009)*. See also *Fair Housing Council of San Francisco Valley v. Roommates.com LLC*, the Ninth Circuit which introduced the "material contribution" test to determine when an online service provider operates beyond the protections of §230 *(521 F.3d 1157, 2008, p. 1162)*.[12]

Courts have not yet decided whether or how §230 may be used as a defence against claims based on outputs from generative AI systems, but recent cases have raised these issues. For example, one lawsuit against OpenAI alleges that its program, ChatGPT, provided a media journalist with defamatory content about the plaintiff based on a fictitious legal complaint generated entirely by the platform itself *(Mark Walters v. OpenAI, LLC, 2023)*. In another case, a plaintiff sued Microsoft, alleging that the company's search engine returned an AI-generated summary conflating the plaintiff's identity with that of a convicted terrorist by a

[12] Observing that a website may avoid liability under Section 230(c)(1) for "passively display[ing] content that is created by third parties," but such website could be subject to liability for "content that it creates itself".

similar name *(Jeffery Battle v. Microsoft Corporation, 2023)*. Although §230 has not been used as a defence in either case, courts may soon need to decide whether generative AI outputs are considered third-party or original content.

Congress introduced legislation to circumvent the immunity provided to online service providers under §230. The *Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act* seeks to explicitly remove §230's blanket immunity from liability for violations of federal civil and state criminal and civil CSAM laws *(EARN IT Act, 2023)*. It also establishes a *National Commission on Online Child Sexual Exploitation Prevention* to develop best practices for online service providers, strengthen enforcement of CSAM laws, and enhance civil remedies for victims. The *Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment (STOP CSAM) Act,* expands reporting requirements for online service providers and allows victims to sue them over CSAM-related harm *(STOP CSAM Act, 2024)*. Providers found violating these provisions could face substantial fines and civil liability.

Two additional bills— the *Children and Teens' Online Privacy Protection Act (COPPA 2.0, 2023)* and the *Kids Online Safety Act (KOSA, 2023)*—are advancing through Congress, both of which target children's online privacy and safety concerns. Together, these reforms signal a growing effort to hold platforms accountable for harm to children while increasing transparency and privacy protections for young users.

Non-consensual Distribution of Intimate Images & Unauthorised Digital Replicas – Federal Level

A variety of laws are available or are being currently considered at both the state and federal levels to protect individuals from the unauthorised use of their likeness and non-consensual image distribution, including statutes that specifically address the growing threat of so-called “deepfakes.”[13] The future adoption of right of publicity legislation on a federal level will create the legal grounds for prosecuting and addressing non-consensual AI-generated deepfakes. Federal Copyright and consumer protection laws may also offer victims some protection, but these laws are narrowly applied.

At the federal level, there is no criminal statute directly targeting the distribution of non-consensual sexual images.[14] However, on March 15, 2022, Congress created a new federal civil claim relating to the publication of intimate images in §1309 of the *Violence Against Women Act Reauthorization Act of 2022 (VAWA),* passed as part of the *Consolidated Appropriations Act, 2022,* making it the first federal law to target the unauthorised distribution of intimate images of both adults and children *(P.L. 117-103, 2022)*. §1309 protections may apply to AI-generated depicting actual, identifiable minors, but not purely imaginary children. Under the provision, victims of morphed CSAM can bring a federal claim against individuals who knowingly—or with reckless disregard as to consent—distribute their images to seek recovery of monetary damages and to enjoin the defendant from further distributing their image *(15 U.S.C. §6851)*.

[13] The term “deepfake” was coined in late 2017 by a Reddit user who created a website for sharing pornographic videos that used open-source face-swapping technology. The term has since expanded to include realistic-looking images of people that do not exist. *See* Meredith Somers, Deepfakes, explained, MIT Management Sloan School (Jul. 21, 2020), https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

[14] Of course, distribution of such material over the internet could violate laws relating to child sexual exploitation and, in circumstances involving threats, extortion, or harassment, could constitute other federal crimes. At least 17 states, including California, Connecticut, Florida, Hawaii, Illinois, Louisiana, Massachusetts, Mississippi, New Jersey, New York, North Carolina, Oklahoma, Rhode Island, Texas, Utah, Washington, and Wyoming, have enacted laws that specifically target impersonation carried out with the intent to intimidate, bully, threaten, or harass a person through social media, email, or other online communications. As of July 1, 2024, it is also a crime in Idaho and Iowa to use explicit synthetic media to harass, humiliate, or engage in blackmail.

Congress has introduced several bills to address the unique risks posed by emerging AI technologies, many of which expressly apply liability for online service providers under certain circumstances. Noteworthy legislative proposals include the *No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act (No AI FRAUD, 2024)*, the *Nurture Originals, Foster Art, and Keep Entertainment Safe Act of 2024 (NO FAKES, 2024)*, and the *Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024 (DEFIANCE, 2024)*. These legislative efforts aim to address the exploitation of digital replicas and the psychological, reputational, and privacy harms associated with the non-consensual disclosure of AI-generated sexual imagery.

Copyright Law

Under the Copyright Act, copyright owners are granted exclusive rights, e.g. right to reproduce their work and create derivative works *(17 U.S.C. §102(b))*. AI-generated images that incorporate or manipulate pre-existing copyrighted material—may infringe upon these exclusive rights and provide the grounds for a copyright infringement claim. However, copyright law does not protect an individual's identity in and of itself, if an image of the individual, i.e. child, is included as a replica in the material.

Courts have begun to address the intersection of copyright law and AI-generated content, shedding light on how these claims might apply to AI-generated CSAM. In August 2023, the U.S. District Court for the District of Columbia issued a first-of-its-kind federal court decision in *Thaler v. Perlmutter, et al. (2023)*, upholding a refusal by the U.S. Copyright Office's (USCO) to register a work created entirely by an algorithm designed by the plaintiff, Dr. Stephen Thaler. The Court rejected the plaintiff's argument that copyright's adaptability to new technologies is expansive enough to contemplate AI authorship. In response to the ruling, the USCO clarified that it will register works partially created with AI, provided a human is credited as the author, but not works wholly generated by AI *(United States Copyright Office, 2023, p.16190)*.

Several high-profile cases have also focused on copyright infringement involving the training of AI models. For example, comedian Sarah Silverman and the *New York Times* sued OpenAI, alleging that their copyrighted works were unlawfully used to train the company's language model *(Paul Tremblay, et al. v. OpenAI, Inc. et al., 2024; The New York Times v. Microsoft Corp., OpenAI, Inc., et al., 2023)*. Additionally, in July 2024, Getty Images filed a lawsuit against Stability AI, accusing it of copying over 12 million photographs and associated metadata to build a competing business model *(Getty Images Inc. v. Stability AI, Ltd., et al., 2024)*. Although many of these cases, and others like them, are ongoing, their outcomes will likely shape the legal framework surrounding the use of copyrighted material in AI systems. The resulting precedents will help determine the liability of platforms that use copyrighted input to train AI models, particularly in cases involving synthetic content.

Consumer Protection Law

The Federal Trade Commission (FTC) plays a critical role in consumer protection *(15 U.S. Code § 45(a)(1))* The FTC has affirmed that AI technologies are not exempt from oversight (Federal Trade Commission, 2023). In fact, the FTC recently published a *Final Rule on Impersonation of Government and Businesses*, which allows the agency to recover consumer redress from those who impersonate government agencies and businesses or to seek civil penalties against those who violate the Rule (Federal Trade Commission, 2024). Now, the agency is considering additional amendments to expand the Rule's scope to cover the impersonation of individuals through digital replicas and voice cloning technologies (Supplemental Notice of Proposed Rulemaking, 2024). Another key element of the proposal is the introduction of "means and instrumentalities" liability, which holds companies accountable if they knowingly or recklessly provide tools, services, or technologies used to facilitate illegal activities. This provision has significant implications for addressing AI-generated CSAM. It would enable the FTC to pursue platforms and developers that fail to implement safeguards, particularly when their tools are misused to create or distribute explicit content involving minors. Expanding liability to AI service providers and developers could reshape the regulatory landscape, influencing how AI tools are developed, deployed, and controlled to prevent exploitation. Proposed legislation in this area underscores the importance of aligning technological innovation with robust protections against misuse.

Non-consensual Distribution of Intimate Images & Unauthorised Digital Replicas – State Legal and Regulatory Frameworks

Statutory and Common Law Privacy Torts

Deepfakes violate personal privacy by exploiting an individual's likeness without consent. When deepfakes involve children, the invasion of privacy is particularly severe. Given the profound violations involved, privacy torts—particularly false light and appropriation of likeness —are considered a critical tool in countering image-based abuse.

At least 9 states and 1 U.S. territory explicitly recognise false light as a distinct privacy tort.[15] Under the Second Restatement of Torts, which most states have adopted, liability for false-light invasion of privacy arises when someone "gives publicity to a matter concerning another that places [them] before the public in a false light," if the false light is "highly offensive to a reasonable person," and if "the actor had knowledge of or acted with reckless disregard for the falsity." (Restatement (Second) of Torts §652E, 1977; McCarthy & Schechter, 2024[16]) To place someone in a false light does not necessarily require an explicitly false statement, but rather misleading impressions that an average person would find highly offensive or objectionable.

A related tort, invasion of privacy by appropriation, involves the "appropriation of the plaintiff's identity or reputation, or some substantial aspect of it, for the defendant's own use or benefit." (Dobbs, Hayden, & Bublick, 2024). However, courts have interpreted this tort inconsistently.

Right of Publicity

The term "Right of Publicity" was first recognised by the Second Circuit in *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc*. Today, 37 states recognise the right of publicity through statute, common law, or both.[17]

[15] These include Arizona, California, D.C., Georgia; Illinois, Indiana, Michigan, New Jersey, Ohio, and Pennsylvania.

[16] Original quote "The courts uniformly adopt the Restatement of Torts list of elements."

[17] States that only have a statutory right include: Arkansas, Hawaii, Illinois, Indiana, Louisiana, New York, Rhode Island, South Dakota, Nevada, Nebraska, and Virginia.

Like the statutes and common law upon which they rely, right of publicity claims differ considerably across jurisdictions, both in what the right protects and how it is protected.

With regards to secondary liability, most state statutes do not specify rules for this. Courts have applied ordinary tort law principles of aiding and abetting liability to find a party liable if they had knowledge of illegal acts and provided substantial assistance in furtherance of those acts (e.g., *Perfect 10, Inc. v. Cybernet Ventures, Inc., 2002; Keller v. Elecs. Arts, Inc., 2010*[18]*)*.

In the context of AI, the right of publicity could be a critical legal tool, with states amending their laws or enacting new ones specifically to cover AI-generated content. Notable examples include California, New York, and Tennessee. Several states, including Illinois, Kentucky, and Louisiana, have also proposed laws targeting AI-generated digital replicas.

Courts have already begun to hear First Amendment challenges involving right of publicity claims in the context of AI. Notable examples include *Andersen v. Stability AI Ltd*. (2023), and *In re Clearview AI, Inc. Consumer Privacy Litigation* (2022). These cases highlight the growing reliance on right of publicity laws to address AI-driven misappropriation of identity. With the advent of more state legislation on the matter, the number of right of publicity claims in relation to content generated by AI is expected to increase.

Non-consensual Distribution of Sexual Images

[18] This allows civil conspiracy claims for violation of California right of publicity to proceed based on defendant’s alleged direction of users to infringing websites.

On the matter of non-consensual distribution of AI-generated sexual images and videos, states have proposed or enacted legislation to tackle this growing phenomenon. Virginia became the first state to amend its “revenge porn” law to include sexual deepfakes *(VA. CODE ANN. § 18.2-386.2, 2019)*.[19] Violations of this statute can result in up to a year in jail, a $2,500 fine, or both. California followed suit in 2019 *(AB 730, 2019-2020)*, followed by Hawaii *(SB 309, 2020 – 2021)* and Georgia *(SB 78, 2021-2022)* in 2021.

In 2022, South Dakota made it a misdemeanour to create non-consensual deepfake pornography, elevating the offense to a felony if the victim is under 17 and the perpetrator is at least 21 *(SD CODE § 22-21-4, 2022)*. Florida passed a law prohibiting the dissemination of non-consensual sexual deepfakes, with violations punishable as a third-degree felony *(SB 1798, 2022)*. The momentum continued in 2023, with 5 states–Illinois, California, Texas, New York, and Minnesota–passing laws to address deepfakes *(SB 382, 2023-2024; CA CODE § 1708.85; SB 1361, 2023; SB S1042A, 2023-2024; HB 1370, 2023-2024)*.

In 2023, state laws also began to distinctly focus on deepfakes/AI-generated content depicting children, with states like Louisiana and Texas making relevant additions to their existing CSAM laws *(SB 175, 2023; HB 2700, 2023)*. In 2024, an additional 11 states including Idaho, Mississippi, South Dakota, Tennessee, Washington, Florida, Kentucky, Oklahoma, Iowa, Georgia, and Virginia enacted laws explicitly adding AI-generated content to their CSAM statutes.

At least 5 states-California, Florida, Illinois, Indiana, and Minnesota–have also implemented civil remedies and private rights of action in response to the distribution of non-consensual sexually explicit deepfakes. In states without such

[19] The update added “falsely created videographic or still image” to the existing language.

provisions, victims of AI-generated intimate images may still be able to seek damages for privacy-related tort claims.

Overall, 49 states and 3 U.S. territories have enacted laws addressing deepfake images and videos, criminalising varying acts around distribution. 19 states specifically prohibit the creation of AI-generated CSAM[20], and 11 states cover both the creation and distribution of non-consensual sexual deepfakes, including AI-generated CSAM.[21] South Carolina remains the only state that has yet to pass such legislation.

To date, state courts in at least 8 states– California, Illinois, Indiana, Minnesota, Montana, Texas, Vermont, and Wisconsin–have adjudicated First Amendment challenges to their states' revenge porn laws and none have ultimately been struck down as unconstitutional.

These decisions did not address the potential interaction between these state laws and §230 of the *Communications Decency Act*, which protects providers and users of interactive computer services from civil or state law claims involving third-party content they did not create or develop.

As of October 2024, at least 37 states are considering legislation targeting the creation and distribution of non-consensual sexual deepfakes (National Conference of State Legislatures, 2024b).

[20] These states include California, Florida, Georgia, Illinois, Iowa, Kentucky, Louisiana, Maryland, Mississippi, New Hampshire, North Carolina, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, Washington, and Wisconsin.

[21] Those states are Alabama, Arizona, Colorado, Delaware, Hawaii, Idaho, Indiana, Massachusetts, Minnesota, New York, and Vermont.

Tech Legislation: AI Governance & Accountability

In recent years, there has been a surge in AI-related legislation at both the state and federal levels, covering a range of regulatory issues such as privacy, transparency, accountability, and consumer protection, carrying significant implications for combating AI-generated CSAM. The cross-border element of AI products and services results in a patchwork of regulations that may negatively impact protection. A unified federal approach could be more appropriate here, to set clear rules and guidelines, providing a unified response to risks arising from AI for child safety.

i. The Federal Regulatory Framework

One of the earliest federal efforts to promote trustworthy AI systems was the *National Artificial Intelligence Initiative Act of 2020,* which tasked the National Institute of Standards and Technology (NIST) with developing an AI Risk Management Framework *(HR 6216, 2019-2020)*. The framework aims to help individuals, organisations, and society manage the risks associated with AI while promoting responsible development and use. The NIST released the *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* in July 2024, offering voluntary guidance on mitigating AI risks (NIST, 2024).

The White House Office of Science and Technology Policy (2022) took this guidance a step further with its *Blueprint for an AI Bill of Rights*. This document identifies five key principles to guide the design, deployment, and use of AI systems: (1) safe and effective systems, (2) protections against algorithmic discrimination, (3) data privacy, (4) notice and explanation, and (5) human alternatives, consideration, and fallback options. Notably, it emphasises that AI systems should undergo rigorous pre-deployment testing, risk identification and mitigation, and continuous monitoring to ensure safety, effectiveness, and compliance with industry standards and to prevent harmful outcomes.

The recently issued *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (White House, 2023b) serves to coordinate efforts across the federal government to promote responsible innovation, protect privacy and civil liberties, safeguard American workers, and manage the risks posed by AI. These initiatives help advance ethical AI practices and ensure that AI is developed and utilised responsibly across the US.

The "Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act"—commonly known as the TAKE IT DOWN Act—was signed into law on May 19, 2025, marking a significant advancement in federal efforts to combat the spread of non-consensual intimate imagery (NCII), including AI-generated deepfakes. This legislation introduces both criminal and civil liabilities, targeting individuals who disseminate such content and imposing obligations on online platforms that host user-generated content.

Under the Act, it is a federal offense to knowingly publish or threaten to publish non-consensual intimate visual depictions of another, whether authentic or AI-generated. For offenses involving adult victims, individuals may face up to two years of imprisonment; if the victim is a minor, the penalty increases to a maximum of three years.

The Act also mandates that “covered platforms”—defined as websites, online services, applications, or mobile applications that primarily host user-generated content—establish and implement notice-and-removal procedures within one year of the law’s enactment. Upon receiving a valid removal request, which must include specific information, such as the individual’s signature and a statement of non-consent, platforms are required to remove the reported content within 48 hours. Failure to comply with these requirements constitutes a violation of the Federal Trade Commission Act and subjects the platform to enforcement actions by the Federal Trade Commission (FTC).

Importantly, the Act provides a “safe harbour” for platforms that act in good faith to remove reported content. This means that if a platform removes content based on a valid request, it is shielded from liability even if the content is later determined not to violate the Act. This provision encourages platforms to act promptly on removal requests without fear of legal repercussions for erroneous takedowns, provided their actions are in good faith.

While the Act represents a comprehensive approach to addressing the challenges posed by the online dissemination of non-consensual intimate imagery, its application to AI-generated CSAM is limited. Notably, the Act is framed around non-consensual intimate images of *identifiable individuals*. Under existing federal law 18 U.S.C. § 2256(8)(C), morphed or computer-manipulated images that use identifiable images of real children fall within the definition of CSAM, and thus the Act would apply to such images. If the image is entirely synthetic and does not depict a real, identifiable child, it would not meet the definition for removal under this Act. Moreover, the Act targets visual content and thus is not designed to reach training sets or synthetic images even if the underlying material contained actual child abuse content.

The State Regulatory Frameworks

Jurisdictions across the United States are increasingly enacting or exploring legislation to address the growing risks posed by AI. In 2024 alone, 45 states and 3 U.S. territories (Puerto Rico, the U.S. Virgin Islands, and Washington D.C.)

introduced over 300 AI-related bills (National Conference of State Legislatures, 2024a). To date, more than 31 states and 2 U.S. territories (Puerto Rico and the U.S. Virgin Islands) have passed laws or adopted resolutions focused on regulating the design, development, and deployment of AI systems (ibid.).

At least 12 states— California *(AB 302, 2023)*, Connecticut *(Public Act No. 23-16)*, Florida *(SB 1680, 2024)*, Illinois *(HB 3563, 2023)*, Louisiana *(HCR 66, 2024)*, New York *(SB 3971, 2019-2020)*, Oregon *(H4153, 2024)*, Pennsylvania *(HR 170, 2024)*, Rhode Island *(SJR 14, 2024)*, Texas *(HB 2060, 2023)*, Utah *(SB149, 2024)*, Vermont *(HB 378, 2018)*, and Washington *(SB 5838, 2024)* — have prioritised the protection of individuals from the unintended impacts of unsafe or ineffective AI systems by forming task forces, advisory councils, and committees to assess AI's impact on consumers and report findings to their governors regarding emerging effects and potential risks of these systems. For example, Vermont created the Division of Artificial Intelligence within the State Agency of Digital Services. Washington's task force is charged with identifying the benefits and risks of AI systems *(SB 5838, 2024)*. Several of these bodies have also been tasked with recommending legislation or regulations to ensure the responsible design, development and use of AI.

Pending legislation in New York seeks to establish an Artificial Intelligence Bill of Rights, granting residents rights and protections to ensure that AI systems operate lawfully, transparently, and with meaningful oversight *(SB 8209, 2024)*. Meanwhile, New Jersey and Massachusetts have introduced bills proposing the creation of a task force as well as a dedicated state department to address the challenges posed by deepfake technology and to mitigate the associated harms to their citizens *(HB 72, 2023-2024; SB 2545, 2024)*.

Several states have passed legislation to protect consumers from abusive data practices, ensuring that consumers are able to control how AI systems collect and use their data.[22] Colorado's legislation stands out by requiring developers of high-risk AI systems to prevent algorithmic discrimination and disclose AI use to consumers *(SB21-190, 2021)*.

At least 12 states — California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Virginia, and Washington—have passed laws to hold AI developers and deployers accountable for non-compliance with AI regulations *(RSC 1985, c C-46, s 163(8))*. For example, Tennessee has implemented data privacy measures related to profiling and requires developers to conduct impact assessments to identify potential negative outcomes from AI-generated decisions, with enforcement authority granted to the state's attorney general, who can impose civil penalties for violations *(HB 1181, 2023)*. Virginia is exploring legislation that would create operating standards for AI system developers and deployers and grant enforcement power to the Office of the Attorney General *(H747, 2024)*. Similarly, Rhode Island has proposed legislation that would require companies that develop or deploy high-risk AI systems to conduct annual impact assessments and adopt comprehensive risk management programs *(H7786, 2024; H 7521/S 2888, 2024)*.

In response to growing concerns over AI-generated explicit content, states such as California *(AB 2273, 2023-2024)*, Utah *(SB 287, 2023)*, Arkansas *(Act 689, 2023)*, Virginia *(SB 1515, 2023-2024)*, Mississippi *(SB 2346, 2023)*, and Louisiana *(HB 142, 2022)* have enacted stricter age-verification requirements for platforms hosting explicit material. Notably, Utah and Arkansas expanded their definitions of

[22] These states include California (California Consumer Privacy Act of 2018, 1798.100 - 1798.199.100), Colorado (SB21-190, 73rd Gen. Assembly (2021)), Connecticut (Public Act No. 22-15*)*, Delaware (HB 154, 152nd Gen. Assembly (2023)), Indiana (SB5, 2023 Leg. Sess.), Iowa (SF 262, 2023 Leg. Sess.), Montana (SB 384, 2023 Leg. Ses.), Oregon (SB 619, 2023 Leg. Sess.), Tennessee (HB 1181, 2023 Leg. Sess. (Pub. Ch. 408)), Texas (HB4, 88th Leg. Sess. (2023), Utah (S148, Artificial Intelligence Policy Act, 2024 Leg. Sess.), and Virginia (SB1392, Consumer Data Protection Act, 2021 Leg. Sess.).

regulated content to encompass AI-generated or simulated sexual acts. However, Arkansas's law was ultimately blocked by a federal court, which ruled that it violated the First Amendment's free speech guarantees *(Netchoice, LLC., v. Tim Griffin, 2023)*.[23] California recently passed its *Safe and Secure Innovation for Frontier Artificial Intelligence Models Act*, which, among other things, requires developers to implement cybersecurity safeguards, conduct harm assessments, engage third-party auditors for compliance, and offers whistleblower protections for employees reporting non-compliance *(SB 1047, 2023-2024)*.

As new state AI regulations emerge, a key challenge has been defining what constitutes a "developer" of an AI system, with particular emphasis on the question of whether modifying or fine-tuning a model turns a user into a developer subject to regulation. In Colorado, the law defines a "developer" as anyone who "intentionally and substantially modifies an AI system," with substantial modification meaning a deliberate change that creates a "reasonably foreseeable risk of algorithmic discrimination."*(SB 205, 2024)* Meanwhile, California's law uses a computational threshold to define a developer as anyone who performs the initial training of a model or fine-tunes a model with a significant amount of computing power *(SB 205, 2024)*. This approach focuses more on the scale of the modifications than their risk of harm. An ideal definition should combine both state models and expand the language to include modifications that create a reasonably foreseeable risk of harm to children.

[23] Netchoice, LLC., v. Tim Griffin, NO. 5:23-CV-05105, U.S. District Court, Western District of Arkansas, Fayetteville Div. (Aug. 31, 2023) (holding that the law was vague and overbroad in violation of Arkansas' First Amendment rights).

Conclusion and Recommendations

The legal framework in the United States for addressing AI-generated CSAM involves a complex and evolving interplay of federal and state laws, regulatory requirements, and proposed legislative reforms. Federal laws governing “child pornography” and “obscenity” are relatively robust, but they are constrained by U.S. Supreme Court precedent, which is both silent on morphed images and explicitly prohibits the criminalisation of synthetic CSAM under the First Amendment. Civil remedies, though significant, are limited in scope and may not adequately address conduct that, despite being harmful, falls short of the legal definition of “child pornography”. Copyright and consumer protection laws may also provide potential avenues for redress, though only in specific and limited circumstances.

The landscape is more fragmented at the state level, with a patchwork of criminal and civil laws that could potentially cover AI-generated CSAM. However, outdated definitions of “child pornography” fail to reach broader forms of digital exploitation, though recent trends indicate a movement toward more inclusive and adaptive legal standards. Statutory and common law privacy torts—such as false light and appropriation of likeness— and right of publicity laws have emerged as potential mechanisms for victim redress, as have laws relating to the non-consensual distribution of sexual images. Nevertheless, these civil frameworks are underdeveloped, leaving significant gaps in accountability for users, developers, distributors, and third-party beneficiaries.

Despite recent legislative efforts to address these legal gaps, U.S. law remains insufficient to address the unique challenges posed by generative AI technologies. Ambiguities in statutory language and constitutional constraints complicate enforcement efforts, with effectiveness largely contingent on prosecutorial discretion and judicial interpretation.

In conclusion, while existing CSAM laws in the U.S. provide a strong foundation of accountability, these statutes were crafted long before generative AI tools gained their foothold online and are clearly insufficient to meaningfully combat the unique dangers posed by these technologies and their outputs. As such, the US face significant challenges in prosecuting and regulating AI-generated CSAM due to constitutional constraints, inconsistent and ambiguous statutory language, and the complexity of enforcing laws in a rapidly evolving technological landscape.

These legal ambiguities underscore the urgent need for a comprehensive regulatory framework that addresses the complexities of AI-generated CSAM. As technology continues to outpace existing laws, the gaps highlighted by cases like *Ashcroft* reveal the limitations of traditional statutes in effectively managing the distinct risks associated with synthetic content. To close these gaps and provide clearer guidance for enforcement, lawmakers must consider targeted reforms that not only clarify the status of AI-generated CSAM under “child pornography” and obscenity laws but also address the underlying technological and ethical issues that drive demand for harmful content. The following recommendations propose a series of reforms to modernise existing legal frameworks, ensuring they remain effective against future technological developments:

Recommendation 1: Amend Existing CSAM Laws to Explicitly Cover AI-Generated Content

Current CSAM laws were crafted long before the advent of AI technologies, leaving significant gaps in their applicability to synthetic content such as deepfakes, morphed images, and other AI-generated material. U.S. statutes, including the PROTECT Act, provide a foundation for criminal liability, but these laws must be updated to explicitly address synthetic CSAM and non-visual depictions.

In the U.S., state-level laws should, at a minimum, adopt language akin to the PROTECT Act, which criminalises the possession and distribution of content that is “indistinguishable” from a real child or is “intended to cause another to believe” that a child is depicted in explicit conduct. For instance, New Hampshire’s recently updated law, effective January 1, 2025, covers images that a reasonable person would conclude are of a child. Similarly, Florida has defined "generated child pornography" as any content created, altered, or modified to depict a fictitious person resembling a real minor engaged in sexual conduct.

Federal and state laws should also explicitly encompass AI-generated images, moving beyond language focused solely on “computer-generated” imagery. For example, 18 U.S.C. § 2252A in the U.S. could be revised to cover content created or manipulated using AI, where minors appear to be engaged in explicit conduct, regardless of the involvement of actual children. Tennessee’s recent legislation provides a model, defining “artificial intelligence” as machine-based systems that make decisions, predictions, or create content without human oversight, including generative AI systems capable of producing realistic imagery or videos.

Recommendation 2: Amend CSAM Laws to Regulate Model Weights and the Misuse of AI Tools

Reforms must also target unregulated datasets and model weights used to generate synthetic CSAM, which are currently outside the scope of U.S. “child pornography” laws which only cover “visual depictions”. To close this loophole, CSAM laws should be amended to explicitly include datasets and model weights within the definition of CSAM and to ban the use of datasets containing CSEA, whether in the form of images or audio recordings, for training AI models. This prohibition should require AI developers to verify and document that datasets are free from harmful or exploitative material.

Additionally, CSAM laws should be amended to criminalise the possession and distribution of model weights trained on CSAM. A practical approach would involve classifying AI models trained on illicit datasets as instruments of abuse, similar to laws governing dual-use technologies such as wiretapping devices or software that circumvents copyright protections which serve as a “proximate link” to the crime. The law should also extend to criminalising the creation and distribution of guides or instructions for generating AI-based CSAM.

Moreover, CSAM laws should establish strict liability for AI developers and companies whose models, knowingly or through negligence, contribute to the creation of distribution of CSAM including via the distribution of model weights created with unvetted training data.

Recommendation 3: Establish a Legally Binding Framework for Safe and Responsible AI Development and Deployment

Effective AI governance requires the establishment of a legally binding framework for safe and responsible AI development and deployment. To prioritise child safety, this framework should delineate key operational standards for developers and online service providers. These standards may include designing AI models with built-in safeguards, such as biasing algorithms against generating CSAM and embedding mechanisms to detect language or prompts commonly associated with misuse. High-risk AI models should undergo mandatory pre-release audits and a certification process, similar to protocols in the pharmaceutical and financial sectors, to assess potential risks, including the capacity to generate CSAM, before deployment.

Developers should also be required to increase transparency by disclosing the metadata and datasets used in AI model training. Online service providers, in turn, must publish annual reports detailing their content moderation practices, conduct safety audits following harmful incidents, and face temporary suspension if they fail to mitigate risks effectively. Continuous auditing and moderation of AI-generated content should be mandatory to prevent the circulation of harmful material on these platforms. Measures should include filtering search terms associated with CSAM, and suspending accounts distributing abusive content.

Such a framework would promote accountability and ensure that AI technologies are developed and deployed responsibly, prioritising child safety at every stage.

Recommendation 4: Expand Legal Protections to Include Control Over One’s Own Image

The U.S. should amend existing privacy laws or adopt new legislation that grants individuals the right to control the use of their image and likeness. With the proliferation of digital technologies and AI-driven media, unauthorised use of a person’s likeness has become easier and more damaging. Expanding privacy protections to include control over one’s image and likeness would allow individuals to prevent misuse, such as the creation and distribution of non-consensual synthetic media or deepfakes. Such protections would support personal and reputational rights, ensuring dignity, autonomy, and control over one’s digital identity.

Alternatively, or in addition to privacy laws, several key changes to copyright laws could be adopted to support victim redress in cases of AI-generated CSAM. First, copyright laws could be revised to allow for the transfer of ownership from offenders to victims through plea agreements or civil settlements, granting victims control over unauthorised AI-generated images depicting their likeness. This approach is akin to the government's authority to seize contraband and can inform this novel approach. By granting copyright ownership to victims, they would gain the right to pursue damages, issue takedown requests, and prevent further use of their likeness in exploitative materials.

To strengthen protections against the exploitation of minors, copyright laws could also be amended to grant children inherent ownership over their own image, thereby providing them exclusive control over unauthorised uses, particularly in cases involving AI-generated content, deepfakes, or synthetic media. New language could be added to existing laws as follows: "Notwithstanding any other provision to the contrary, ownership rights in an image shall not extend to photographs or likenesses of a minor, who shall possess an automatic right to control the use of their image." Additionally, provisions related to infringement could be amended to add "any individual who captures or publishes a photograph or likeness of a minor shall be liable for infringement of the minor's image rights. The minor shall be entitled to pursue all remedies available under this title for such infringement." To balance these protections with practical considerations, the amendment could establish exceptions including for personal or family use, express consent, and incidental capture. This measure would allow children and their guardians to prevent the distribution or misuse of their likeness in harmful ways.

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/

USA

14 V.I.C. § 489

15 U.S.C. § 45(a)(1) (2024)

15 U.S.C. § 6851 (2024)

17 U.S.C. §106

18 PA. CONS. STAT. §3051

18 U.S.C. (1996)

18 U.S.C. § 2256(8)(B)(1)–(2) (1996)

18 U.S.C. § 2258A(a)(2)(A) (2024)

42 PA. STAT. AND CONS. STAT. § 8316(d) (2024)

720 ILCS 5/11-20

720 ILL. COMP. STAT. 5/11-20.1(4),(f)(7)

765 ILL. COMP. STAT. 1075/5.

AB 1831, 2023–2024 Leg. Sess. (Sep. 29, 2024)

AB 1863, CA Leg. Sess. (2023-2024)

AB 2273, The California Age-Appropriate Design Code Act, Leg. Sess. (2023-2024)

AB 2602, CA Leg. Sess. (2023-2024)

AB 302. (2023). An act to add Section 11546.45.5 to the Government Code, relating to automated decision systems. 2023 Legislative Session

AB 730, 2019-2020 Leg., Reg. Sess.

Act 689 of 2023

AK STAT § 11.61.127(a)

AK STAT. §09.55.650

AL ST § 13A-12-194

AL ST §13A-6-240

Allison v. Vintage Sports Plaques, 136 F.3d 1443 (11th Cir. 1998)

Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018)

Almeida v. Amazon.com, Inc., 456 F.3d 1316 (11th Cir. 2006)

American Law Institute. (1977). Restatement (Second) of Torts § 652I

Anderson v. Fisher Broad. Co., 712 P.2d 803 (Or. 1986)

ARK. CODE ANN. § 5-27-602(a)(1)

Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002)

Association Services v. Smith, 549 S.E.2d 454, 459 (Ga. Ct. App. 2001)

AZ STAT § 13-3553

AZ STAT. §§ 12-761, 13-3726

Bullard v. MRA Holding, LLC, 740 S.E.2d 622 (Ga. 2013)

CA PENAL § 311.11

CAL. CIV. CODE §§ 3344(f), 3344.1(a)(l) (West 2024)

California Code § 1708.85

California Consumer Privacy Act of 2018, §§ 1798.100 - 1798.199.100

Children and Teens' Online Privacy Protection Act (COPPA 2.0), S.1418, 118th Congress (2023-2024)

Comedy III Prods. v. Saderup, 21 P.3d 797 (Cal. 2001)

Communications Act of 1934, 47 U.S.C. § 151 et seq. (1934)

Communications Decency Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 56 (1996)

CONN. GEN. STAT. § 54-201 et. seq.

Cox v. Hatch, 761 P.2d 556 (Utah 1988)

CT ST § 53a-193

Curran v. Amazon.com, 86 U.S.P.Q.2d 1784 (S.D. W. Va. 2008)

Curran v. Children's Service Center Inc., 578 A.2d 8, 12 (Pa. Super. Ct. 1990)

DEL. CODE ANN. tit. 11, §§ 1100, 1109

Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024, S.3696, 118th Congress (2023-2024)

Dobbs, D. B., Hayden, P. T., & Bublick, E. M. (2024). The law of torts (2nd ed., § 579)

*Doe #1 v. MG Freesites, Ltd., 2022 WL 407147, at *12 (N.D. Ala. Feb. 9, 2022)*

Doe v. Backpage.com, LLC, 817 F.3d 12, 18–24 (1st Cir. 2016)

Doe v. Boland, 698 F.3d 877 (6th Cir. 2012)

Doe v. Mindgeek USA, Inc., 558 F. Supp. 828, 835 (C.D. Cal. 2021)

Doe v. MySpace, Inc., 528 F.3d 413, 420 (5th Cir. 2008)

Does #1-6 v. Reddit, Inc., 51 F4th 1137, 1140–1141 (9th Cir. 2022), cert. denied sub nom., 143 S. Ct. 2560 (U.S. 2023)

Donchez v. Coors Brewing Co., 392 F.3d 1211 (10th Cir. 2004)

Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT Act), 2023, S.1207, 118th Cong. Sess. (2023-2024)

En Banc Observation, 521 F.3d 1157, 1162 (9th Cir. 2008)

Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481 (3d Cir. 1956)

Ex parte Jordan Bartlett Jones, 2021 WL 2126172 (Tex. 2021)

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. (2023b, October 30). *White House*. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

Federal Bureau of Investigation. (2024, March 29). *Child sexual abuse material created by generative AI and similar online tools is illegal*. [Public Service Announcement]. Retrieved from https://www.ic3.gov/PSA/2024/PSA240329.

Federal Trade Commission. (2023, April 25). Joint statement on enforcement efforts against discrimination and bias in automated systems. Retrieved from https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/joint-statement-enforcement-efforts-against-discrimination-bias-automated-systems.

Federal Trade Commission. (2024, April 1). FTC announces impersonation rule goes into effect today. Retrieved from https://www.ftc.gov/newsevents/news/press-releases/2024/04/ftc-announces-impersonation-rule-goes-effect-today.

Fergerstrom v. Hawaiian Ocean View Estates, 441 P.2d 141 (Haw. 1968)

FL STAT § 847.0135(c)

FL STAT. § 960.197

FLA. STAT. §847.01357

FTC v. Accusearch Inc., et al., No. 08-8003 (10th Cir. 2009)

GA. CODE ANN. § 16-12-100.2(b.2)

Getty Images (US), Inc. v. Stability AI, Ltd., et al., No. 23-135 (JLH), U.S. District Court for the District of Delaware (filed July 8, 2024)

Giboney v. Empire Storage & Ice Co., 336 U.S. 490 (1949)

Gignilliat v. Gignilliat, Savitz & Bettis L.P., 684 S.E.2d 756 (S.C. 2009)

Gill v. Curtis Publ'g Co., 239 P.2d 630 (Cal. 1952)

Godbehere v. Phoenix Newspapers, Inc., 783 P.2d 781, 787 (Ariz. 1989)

H 7521, 2024 Leg. Sess.

H.R. 6216, National Artificial Intelligence Initiative Act of 2020, 116th Congress (2019-2020)

H.R.8005 - Child Exploitation and Artificial Intelligence Expert Commission Act of 2024

H4153. (2024). 82nd Legislative Session

H747, 2024 Leg. Sess.

H7786, 2024 Leg. Sess.

Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953)

Hart v. Elec. Arts. Inc., 717 F.3d 141 (3d Cir. 2013)

HAW. REV. STAT. § 707-750

HB 1126, Walker Montgomery Protecting Children Online Act, 2024 Leg. Sess.

HB 1181, Tennessee Leg. Sess. (2023) (Pub. Ch. 408)

HB 1370, 93rd Leg. Sess. (2023-2024)

HB 142, Act No. 440, 2022 Leg. Sess.

HB 154, 152nd Gen. Assembly (2023)

HB 1999, 68th Leg. Sess. (2023-2024)

HB 2060. (2023). 88th Legislative Session

HB 207, 2024 Leg. Sess.

HB 2091, Ensuring Likeness, Voice, and Image Security Act of 2024, 113th Gen. Assembly (2024)

HB 2163, 2024 Leg. Sess.

HB 2700, 88th Leg. Sess. (2023)

HB 3563. (2023). 103rd General Assembly (Public Act 103-0451)

HB 3642, 2024 Leg. Sess.

HB 378. (2018). An act relating to the creation of the Artificial Intelligence Task Force. 2018 Legislative Session

HB 4, Texas Leg. Sess. (2023)

HB 4875, 103rd Gen. Assembly (2023-2024)

HB 575, 67th Leg. Sess. (2024)

HB 72, 193rd Gen. Assembly (2023-2024)

HB 993, 2024 Leg. Sess.

HCR 66. (2024). An act to provide for a joint legislative committee to study regulations regarding AI. 2024 Legislative Session

Hepp v. Facebook, Inc., 465 F. Supp. 3d 491 (E.D. Pa. 2021)

HI REV. STAT. § 712-1210

Hirsch v. S.C. Johnson & Son, Inc., 90 Wis.2d 379 (1979)

Hougum v. Valley Mem'l Homes, 574 N.W.2d 812 (N.D. 1998)

HR 170. (2024). A resolution directing the Joint State Government Commission to establish an advisory committee to conduct a study on the field of artificial intelligence and its impact and potential future impact in Pennsylvania. 2024 Legislative Session.

HR.4123, Child Pornography Prevention Act of 1996, 104th Congress (1995-1996)

IA ST § 728.12

ID STAT § 18-1507

IN CODE § 35-49-1-3(2)

In re Estate of Reynolds, 327 P.3d 213 (Ariz. Ct. App. 2014)

In Re: Clearview AI, Inc., Consumer Privacy Litigation, No. 1:2021cv00135 - 314 (N.D. Ill. 2022)

IND. CODE § 32-36-1-6.

IND. CODE § 35-42-4-4(d)

Jackson v. Roberts, No. 19-480 (2d Cir. Aug. 19, 2020)

Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016)

Jeffery Battle, Battle Enterprises, LLC, v. Microsoft Corporation, No. JRR23CV1822, U.S. District Court for the District of Maryland (Jul. 7, 2023)

KAN. STAT. ANN. § 60-5001

Keller v. Elecs. Arts, Inc., No. 09-cv-1967, 2010 WL 530108 (N.D. Cal. Feb. 8, 2010)

Kids Online Safety Act (KOSA), H.R.7891, 118th Congress (2023-2024)

Kimbrough v. Coca-Cola/USA, 521 S.W.2d 719 (Tex. Civ. App. 1975)

Klayman v. Segal, 783 A.2d 607, 613 (D.C. 2002)

KRS STAT § 21-5510

KY STAT § 531.010

LA STAT. ANN. § 46:1802 et seq.

Lane v. Random House, Inc., 985 F. Supp. 141 (D.D.C. 1995)

Logan v. State, 836 N.E.2d 467 (2005)

Longoria v. Kodiak Concepts LLC, 527 F. Supp. 3d 1085 (D. Ariz. 2021)

Lovgren v. Citizens First National Bank, 534 N.E.2d 987 (Ill. 1989)

Mark Walters v. OpenAI, LLC, Superior Court of Gwinnett County, Georgia (June 2023)

MASS. GEN. LAWS ch. 265, §50

MASS. STAT. ANN. Ch. 214, § 3A (2024)

McCarthy, J. T., & Schechter, R. E. (2024). The rights of publicity and privacy (2nd ed.)

MD CODE § 11-203

MD. CODE §§ 11-207, 208

MI COMP. LAWS § 750.145c (1999)

MICH. COMP. LAWS § 750.145c(b)

Miller v. California, 413 U.S. 15 (1973)

MINN. STAT. § 617.246(f)(2)(i)-(iii)

MINN. STAT. §617.245 (Subd. 2)

MN STAT. ANN. § 617.293

MO. REV. STAT. § 573.01(4)(b)(c)

MO. REV. STAT. §537.047

Moore v. Sun Pub. Corp., 881 P.2d 735 (N.M. 1994)

Morganroth v. Whitall, 411 N.W.2d 859, 863-64 (Mich. Ct. App. 1987)

MS STAT § 97-5-31

MT ST § 45-5-625

MT. CODE ANN. §27-2-216

N.C. GEN. STAT. §14–190.5A(g)

N.H. REV. STAT. ANN. § 21-M:8-h

N.H. REV. STAT. ANN. §633:11

N.J. STAT. ANN. § 2A:30B-3(a). FL STAT. § 960.197

N.J. STAT. ANN. §2A:30B-3

N.M. STAT. ANN. § 31-22-3 et seq

N.Y. CIV. RIGHTS LAW § 50-f(9)

National Conference of State Legislatures. (2024a, September 9). *Artificial Intelligence 2024 Legislation*. Retrieved from https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation.

National Conference of State Legislatures. (2024b). *Deceptive audio or visual media ("deepfakes") 2024 legislation*. Retrieved October 10, 2024, from https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation.

National Institute of Standards and Technology (NIST). (2024, July). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*. U.S. Department of Commerce. Retrieved from https://www.nist.gov/itl/ai-risk-management-framework.

Nature's Way Prods. v. Nature-Pharma, Inc., 736 F. Supp. 245 (D. Utah 1990)

NC STAT ANN. § 14-202.7

NE REV. STAT. § 28-807(7)

NE STAT § 28-1463.02(6)

NEB. REV. STAT. §25-21,292

Nelson v. J.C. Penney Co., 75 F.3d 343 (8th Cir. 1996)

NetChoice, LLC v. Griffin, No. 5:23-CV-05105, U.S. District Court, Western District of Arkansas, Fayetteville Div. (Aug. 31, 2023)

New York v. Ferber, 458 U.S. 747 (1982)

NH REV. STAT. § 649-A-2(I),(IV),(V)

NJ REV. STAT. § 2C:24-4

NM STAT § 30-6A-2

NMI 3116

No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act, H.R. 6943, 118th Congress (2023-2024)

Nurture Originals, Foster Art, and Keep Entertainment Safe Act of 2024, H.R. 9551, 118th Congress (2023-2024)

NY PENAL CODE § 245.15

OHIO REV. CODE ANN. § 2741.02(E) (West 2024)

OK STAT. T. 21, § 1040.56

OKLA. STAT. tit. 21, §1040.56

OR ST §§ 163.686, 163.687

Osborne v. Ohio, 495 U.S. 103, 110 (1990)

Paul Tremblay, et. al. v. OpenAI, Inc, et al., 23-cv-03223-AMO (N.D. Cal. Feb. 12, 2024)

People v. Austin, 155 N.E.3d 439, 448–49 (Ill. 2019)

People v. Iniguez, 202 Cal. Rptr. 3d 237 (Cal. App. Dep't Super. Ct. 2016)

People v. Riggs, 604 N.W.2d 68, 237 Mich. App. 584 (1999)

Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002)

Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 (PROTECT ACT), 108th Leg. Sess., 117 Stat. 650, Pub. L. No. 108-21 (2003)

Prosser, W. L. (1960). Privacy. California Law Review, 48(3), 383-389

PROTECT Our Children Act of 2008, Pub. L. 110-401, Oct. 13, 2008, 122 Stat. 4229 (18 U.S.C. §§ 2258A–2258E; 34 U.S.C. §§ 21101 et seq.)

Pub. L. No. 108-21, 117 Stat. 650 (2003)

Public Act No. 22-15 (2022)

Public Act No. 23-16. (2023)

Public Law 117-103, 2022

R.I. GEN. LAWS § 11-9-1.3(c)(1)(i)-(iii)

R.I. GEN. LAWS §9-1-2

REPORT Act of 2023, Pub. L. 118-59, §§ 3, 4(a), May 7, 2024, 138 Stat. 1016

Ricci v. Teamsters Union Local 456, 781 F.3d 25, 27–28 (2d Cir. 2015)

Romaine v. Kallinger, 537 A.2d 284, 290 (N.J. 1988)

Rosa and Raymond Parks Institute for Self-Development v. Target Corp., No. 15-10880 (11th Cir. 2016)

Roth v. United States, 354 U.S. 476 (1957)

S 2888, 2024 Leg. Sess.

S.D. CODIFIED LAWS §§ 22-24A-8, 22-24A-10

S.D. CODIFIED LAWS §§22-24A-7, 22-24A-10

S148, Artificial Intelligence Policy Act, Utah Leg. Sess. (2024)

SB 1047, Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, Reg. Leg. Sess. (2023-2024)

SB 1361, 2023 Leg., Reg. Sess.

SB 1392, Consumer Data Protection Act, Virginia Leg. Sess. (2021)

SB 149. (2024). 2024 Legislative Session

SB 1515, Reg. Leg. Sess. (2023-2024)

SB 1680, 2024 Leg. Sess.

SB 1680. (2024). 2024 Legislative Session

SB 175, 2023 Leg. Sess.

SB 1798, 2022 Leg., Reg. Sess.

SB 205, 2024 Leg. Sess.

SB 217, 2024 Leg. Sess.

SB 2243, 2023-2024 Leg. Sess.

SB 2346, 2023 Leg. Sess.

SB 2545, NJ Leg. Sess. (2024)

SB 287, 2023 Leg. Sess.

SB 309, 2020-2021 Leg., Reg. Sess.

SB 317, An act relating to commercial rights to the use of names, voices, and likenesses, 2024 Leg. Sess.

SB 382, 2023-2024, 103rd Leg. Sess.

SB 384, Montana Leg. Sess. (2023)

SB 3971. (2019-2020). An act creating a temporary state commission to study and investigate how to regulate artificial intelligence, robotics, and automation; and providing for the repeal of such provisions upon expiration thereof. 2019 Legislative Session

SB 5092, Washington Leg. Sess. (2021-2022)

SB 5838. (2024). Artificial Intelligence Taskforce. 68th Legislative Session

SB 619, Oregon Leg. Sess. (2023)

SB 713, 2024 Leg. Sess.

SB 78, 2021-2022 Leg., Reg. Sess.

SB 79, 99th Leg. Sess. (2024)

SB 8209. (2024). 2024 Legislative Session

SB S1042A, 2023-2024 Leg., Reg. Sess. (codified at NY Penal Code § 245.15)

SB S7676, Digital Replicas Contract Act, NY Leg. Sess. (2023-2024)

SB21-190, 73rd Gen. Assembly (2021)

SB5, Indiana Leg. Sess. (2023)

SC STAT § 16-15-375

SD STAT § 22-24A-2(5),(8)

SF 262, Iowa Leg. Sess. (2023)

Shoemaker v. Taylor, 730 F.3d 778 (9th Cir. 2013)

SJR 14. (2024). 2024 Legislative Session

Somers, M. (2020, July 21). Deepfakes, explained. *MIT Management Sloan School.* Retrieved from https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

South Dakota Code § 22-21-4

St. John v. Town of Ellettsville, 46 F. Supp. 2d 834, 851 (S.D. Ind. 1999)

Stanley v. Georgia, 394 U.S. 557 (1969)

State ex rel LaFollette v. Hinkle, 229 P.317 (Wash. 1924)

State ex rel. Elvis Presley Intern. Mem'l Found. v. Crowell, 733 S.W.2d 89 (Tenn. Ct. App. 1987)

State of Indiana v. Conner Katz, No. 20S-CR-632, __ N.E.3d__ (Ind., Jan. 18, 2022)

State of Vermont v. Rebekah S. VanBuren, 210 Vt. 293 (2018)

State v. Casillas, 952 N.W.2d 629, 634 (Minn. 2020)

State v. Culver, 918 N.W.2d 103 (Wis. Ct. App. 2018)

State v. Lamoureux, 485 P.3d 192 (Mont. 2021)

Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act of 2024, H.R.7949, 118th Congress (2023-2024)

Supplemental notice of proposed rulemaking, 89 Fed. Reg. 15072 (proposed Mar. 1, 2024) (to be codified at 16 C.F.R. pt. 461)

Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act

Tenn. Code § 47-25-1101 et seq. (2024)

TEX. CODE CRIM. PRO. ANN. art. 56b.001 et. seq

Thaler v. Perlmutter, et al., No. 1:2022cv01564, U.S. District Court for the District of Columbia (2023)

The Intimate Image Protection Amendment Act (Distribution of Fake Intimate Images), S.M. 2024, c. 17

The New York Times v. Microsoft Corp., OpenAI, Inc., et al., 1:23-cv-11195 (S.D. NY Dec. 27, 2023)

TN CODE ANN. § 39-17-901(7)

TN STAT § 39-17-1002(2)(E)

TX PENAL CODE § 43.261(b-1)

U.S. CONST. amend. I.

U.S. Department of Justice. (2020, May 28). *Citizen's guide to U.S. federal law on child pornography*. Retrieved from https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography

U.S. Department of Justice. (2024a, May 1). *Recidivist sex offender sentenced for possessing deepfake child sexual abuse material*. Retrieved from https://www.justice.gov/opa/pr/recidivist-sex-offender-sentenced-possessing-deepfake-child-sexual-abuse-material

U.S. Department of Justice. (2024b, May 20). *Man arrested for producing, distributing, and possessing AI-generated images of minors engaged in sexually explicit conduct*. Retrieved from https://www.justice.gov/opa/pr/man-arrested-producing-distributing-and-possessing-ai-generated-images-minors-engaged

United States Attorney's Office, Western District of North Carolina. (2023, November 8). *Charlotte child psychiatrist is sentenced to 40 years in prison for sexual exploitation of a minor and using artificial intelligence to create child pornography images of minors*. Retrieved from https://www.justice.gov/usao-wdnc/pr/charlotte-child-psychiatrist-sentenced-40-years-prison-sexual-exploitation-minor-and

United States Copyright Office. (2023, March 16). Copyright registration guidance: Works containing material generated by artificial intelligence. Federal Register, 88(51), 16190

United States v. Acheson, 195 F.3d 645 (11th Cir. 1999)

United States v. Anderson, 759 F.3d 891 (8th Cir. 2014)

United States v. Arvin, 900 F.2d 1385 (9th Cir. 1990)

United States v. Dost, 636 F. Supp. 828 (S.D. Cal. 1986), aff'd sub nom. United States v. Wiegand, 812 F.2d 1239 (9th Cir. 1987)

United States v. Fox, 248 F.3d 394 (5th Cir. 2001)

United States v. Hilton, 167 F.3d 61 (1st Cir. 1999)

United States v. Hotaling, 634 F.3d 725 (2d Cir. 2011)

United States v. Mecham, 950 F.3d 257 (5th Cir. 2020), cert. denied, 141 S. Ct. 139 (2020)

United States v. Mento, 231 F.3d 912 (4th Cir. 2000)

United States v. Salcido, 506 F.3d 729 (9th Cir. 2007)

United States v. Villard, 885 F.2d 117, 124 (3d Cir. 1989)

United States v. Williams, 553 U.S. 285 (2009)

UT STAT § 76-5b-103(1)(b)(ii), (c), (3)(a)(ii), (b)

UTAH CODE ANN. §77-38-15

VA. CODE ANN. § 18.2-374.1(A)

VA. CODE ANN. § 18.2-386.2 (2019)

VA. CODE ANN. §8.01-42.4

VT. STAT. ANN. tit. 13, § 5451 et seq.

W. & S. Fin. Grp. Beneflex Plan, 797 F. Supp. 2d 796 (W.D. Ky. 2011)

WA STAT § 9.68A.011

WASH. REV. CODE § 7.68.020

WASH. REV. CODE §9.68A.130

Weaver v. Myers, 229 So.3d 1118 (Fla. 2017)

Welling v. Weinfeld, 866 N.E.2d 1051 (Ohio 2007)

White House Office of Science and Technology Policy. (2022, October 4). *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*. Retrieved from https://www.whitehouse.gov/ostp/ai-bill-of-rights/

White House. (2023a, July 21). *Fact sheet: Biden-Harris administration secures voluntary commitments from leading artificial intelligence companies to manage the risks posed by AI*. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

White v. Samsung Electronics America, Inc., 971 F.2d 1395 (9th Cir. 1992)

WI STAT § 948.125(1)(a)

WI STAT. § 949.01 et seq.

WIS. STAT. §948.051

Wood v. Hustler Mag., Inc., 736 F.2d 1084 (5th Cir. 1984)

WYO. STAT. ANN. § 6-4-303(a)(ii)(B)

Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977)

Zeran v. American Online, Inc., 129 F.3d 327, 331–333 (4th Cir. 1997)

More information

Suggested citation: Schidlow, J., Gaitis, K.K., 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? USA. 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].