CHILD USA

PAVING THE WAY FOR JUSTICE AND PREVENTION

LEGAL & REGULATORY FRAMEWORKS FOR ADDRESSING AI-GENERATED CSAM IN THE UNITED STATES & CANADA

Prepared for Childlight Global Child Safety Institute's *Searchlight 2025* study on legal challenges in regulating generative AI CSAM across the Five Eyes nations

2025

Authored By :

Jessica Schidlow, Esq.

Legal Director, CHILD USA

CONTEXT & CONTRIBUTION

This report was prepared as a contribution to the Childlight Global Child Safety Institute's *Searchlight 2025: Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse*. The research contained herein informed the following study: Study F – *Legal Challenges in Tackling AI-Generated Child Sexual Abuse Material Across the UK, USA, Canada, Australia, and New Zealand: Who Is Accountable Under the Law?*

Complete Study

https://www.childlight.org/searchlight/study-f-legal-challenges-in-tackling-ai-generated-child-sexual-abuse-material-across-the-uk-usa-canada-australia-and-new-zealand-who-is-accountable-according-to-the-law

Associated Project

osf.io/as83r

**Research last updated October 31, 2024*

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The widespread accessibility of artificial intelligence (AI) technologies has created unprecedented threats to children's safety. Criminal and malicious actors can now leverage AI tools to produce obscene, abusive, and photorealistic images of children, and they can disseminate this material to thousands, if not millions, of users within a matter of minutes. Generative AI models can even provide offenders with instructional content for grooming, concealing evidence, and coercing victims into silence. As the line between real and synthetic[1] child sexual abuse material (CSAM) becomes increasingly blurred, it raises urgent questions about how existing laws can and must evolve to address the misuse of AI technologies.

To that end, this report evaluates the legal and regulatory frameworks in the United States and Canada to determine how effectively they address criminal and civil liability for the possession, creation, and distribution of AI-generated CSAM. It examines whether existing laws ensure accountability not only for end users, but also for developers, dataset holders, and service providers that enable the proliferation of this content online. In addition, the report analyzes current legislative and regulatory proposals on AI governance, recognizing that the safe and responsible development of these technologies is critical to preventing the future exploitation of children.

Existing laws, initially crafted to combat the hands-on abuse of real children, are ill-equipped to address the distinct challenges posed by generative AI, creating loopholes that offenders exploit to evade detection and accountability. By analyzing these legal gaps and ambiguities, this report seeks to identify critical reforms needed to ensure the law remains effective in the face of rapidly evolving technologies that threaten to harm children in new and deeply troubling ways.

[1] The term "synthetic" CSAM refers to AI-generated photorealistic images of fictitious children. For purposes of this report, the terms "synthetic" and "virtual" CSAM are used interchangeably.

II. METHODS

This report uses a doctrinal legal research methodology, also known as "black letter" methodology, to examine the legal frameworks for CSAM in relation to emerging AI technologies. Using this method, the author 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 therein, and determine necessary legal reforms.

A. DATA AND SOURCES

An initial examination of legal databases and primary sources was undertaken to identify pertinent statutes, case law, and legislative materials relevant to CSAM and AI regulation. Key sources include:

- **Westlaw**: An initial jurisdictional survey was conducted via Westlaw using the platform's advanced search tools and legal index taxonomy to identify CSAM-related laws, including "child pornography" and obscenity statutes, across all 50 U.S. states, territories, and the federal government. Westlaw's advanced search tools were also used to refine queries to capture relevant case law, statutory annotations, and notes of decision on issues such as copyright, common law torts, and consumer protection laws. Secondary sources were also reviewed to provide broader context.

- **Justice Laws Website**: Operated by the Canadian Government, this resource provides access to federal acts and regulations and is updated approximately every two weeks. This site was used to identify applicable Canadian federal statutes, regulations, and current bills under consideration in Parliament. Official press releases and reports linked on the site further informed the research.

- **CanLII Database**: CanLII, a non-profit initiative of the Federation of Law Societies of Canada, offers open access to statutes, regulations, case law, and secondary sources, across Canadian jurisdictions. This database facilitated a review of provincial laws and decisions by the Canadian Supreme Court and various federal and provincial tribunals.

- **National Conference of State Legislatures (NCSL)**: The NCSL database was reviewed to identify pending and enacted legislation specific to AI across U.S. jurisdictions. This allowed for an assessment of legislative trends and ongoing developments in AI regulation.
- **Multistate AI Legislation Tracker**: This tool was reviewed to identify AI-related legislation trends and to compare state-level legislative actions across the U.S.
- **Legiscan**: Proposed bills identified in the NCSL database and through the Multistate tracker were cross-referenced on Legiscan to access complete legislative language or through direct links to congressional websites. Legiscan provides comprehensive access to federal and state bills, allowing detailed tracking of legislative proposals.
- **Additional Sources**: 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/ICMEC database and the OECD database.

B. SELECTION PROCESS

Legislation and case law were selected for inclusion based on their relevance to child sexual exploitation and CSAM, particularly in the context of generative AI software and accountability. All identified statutes, case law, and legislative proposals were organized in Excel for analysis, with equal attention given to both the presence and absence of relevant provisions. This approach allowed for a thorough examination of the strengths and gaps within legal frameworks across the jurisdictions studied.

C. DATA EXTRACTION

Key information regarding statutory definitions, accountability mechanisms, and relevant findings were included in a data extraction tool developed by the Childlight research team consistent with the study's objectives:

- **Definitions**: How federal, state, and provincial laws define terms such as "child pornography," "obscene material," and related offenses, with a special focus on computer-generated or synthetic 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 synthetic 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 ensures a comprehensive review of the current legal frameworks while highlighting areas for potential reform to meet the challenges posed by advancements in AI technology.

III. ANALYSIS: LEGAL AND REGULATORY FRAMEWORKS IN THE UNITED STATES

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"[2] 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 criminalization 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

[2] While the term "child pornography" is still widely used in legal contexts, this report will use the term "child sexual abuse material" (CSAM) except when referencing specific statutory language or criminal offenses as the term CSAM more accurately reflects the nature of this crime.

as potential mechanisms for victim redress, as have laws relating to the nonconsensual 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, the existing U.S. framework 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.

A. "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.[3] Two landmark Supreme Court cases, *Miller v. California* and *New York v. Ferber*, have significantly shaped this framework.[4] These decisions affirm that CSAM and obscenity are categorically excluded from First Amendment protection, granting federal and state governments broad authority to regulate the possession, production, and distribution of these materials.

In *Miller*, the Supreme Court established a three-part test for determining whether material is legally obscene and, therefore, unprotected under the First Amendment. To qualify as obscene, the material must "appeal to the prurient interest in sex" (as judged by contemporary community standards), depict or describe sexual conduct (as defined by state law) in a patently offensive way, and lack "serious literary, artistic, political, or scientific value."[5] Although subjective and ambiguous, the *Miller* test provides an essential foundation for regulating sexually explicit content that does not meet the criminal threshold for "child pornography" but may still be harmful to minors.[6] However, since the test requires a nuanced, case-by-case assessment of the material at

[3] The First Amendment states, "Congress shall make no law **...** abridging the freedom of speech." U.S. CONST. AM. 1.
[4] Miller v. California, 413 U.S. 15 (1973); New York v. Ferber, 458 U.S. 747 (1982); *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").
[5] 413 U.S. 15, 24 (1973).
[6] The First Amendment protects the private possession of obscene material depicting virtual minors, so long as no real children are victimized. *See* Ashcroft v. Free Speech Coal., 535 U.S. 234, 250 (2002); *see also* Stanley v. Georgia, 394 U.S. 557, 559 (1969) (holding that the "mere private possession of obscene matter cannot constitutionally be made a crime.").

issue, the legislature is precluded from using obscenity law as a basis for categorically regulating AI-generated CSAM.

Nine years after *Miller*, the Court in *Ferber* held that the First Amendment does not protect CSAM, regardless of whether the material is considered obscene.[7] Emphasizing the government's compelling interest in child protection, the Court explained that "the use of children as subjects of pornographic materials is harmful to the psychological and emotional health of the child."[8] The Court expanded the state's regulatory authority to cover not only the production of CSAM but also its dissemination, promotion, and exhibition. In doing so, the Court explained that the distribution of such material endangers children by feeding the "distribution network" that perpetuates their exploitation and abuse.[9] Although the *Ferber* Court acknowledged both the direct and indirect harms associated with CSAM, its ruling centered on regulating content that involves *direct* harm to *actual* children, leaving materials that cause only indirect harm beyond the scope of absolute prohibition.

Congress attempted to close this loophole when it passed the *Child Pornography Prevention Act (CPPA)*, which expanded the definition of "child pornography" to include virtual or computer-generated images that "appear to" depict or "convey the impression" of minors engaging in sexually explicit conduct.[10] In *Ashcroft v. Free Speech Coalition*, the Supreme Court struck down these portions of the CPPA as overly broad, finding the possession or distribution of images created by using adults who look like minors or computer-generated images to be beyond the reach of *Ferber*.[11] In *dicta*, the Court discussed the concept of morphed images and, without deciding on the issue, noted that they are closer to the exception created by *Ferber* because they implicate the

[7] *See* New York v. Ferber, 458 U.S. 747 (1982)
[8] Id at 757-58 ("The prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance.").
[9] Id at 748, 760-61.
[10] HR.4123, Child Pornography Prevention Act of 1996, 104th Congress (1995-1996); 18 U.S.C. § 2256(8)(B)(1)-(2) (1996) (defining child pornography as "visual depictions, including any . . . computer-generated image or picture,' that 'is or appears to be, of a minor engaging in sexually explicit conduct," and "any sexually explicit image . . . 'that conveys the impression' it depicts a minor engaging in sexually explicit content.").
[11] 535 U.S. 234, 240 (2002); Before the *Ashcroft* decision, several federal circuit courts upheld the CPPA on constitutional challenges to the new language. *see* United States v. Hilton, 167 F.3d 61, 76-77 (1st Cir. 1999) (holding that CPPA falls outside constitutionally-protected speech and that the CPPA's definition of child pornography is "adequately precise"); United States v. Mento, 231 F.3d 912, 923 (4th Cir. 2000) (same); United States v. Fox, 248 F.3d 394, 411 (5th Cir. 2001); United States v. Acheson, 195 F.3d 645, 650-53 (11th Cir. 1999) (finding that the CPPA language was neither vague nor overly broad).

interests of actual children.[12] Despite the lack of definitive Supreme Court guidance on the issue, federal courts have generally upheld convictions based on morphed images, finding the resulting harm caused by such images significant enough to justify their exclusion from First Amendment protections.[13] Still, the *Ashcroft* decision has created a legal loophole for AI-generated CSAM as such content—while harmful—does not necessarily involve the hands-on abuse of an actual child.

In response to *Ashcroft*, Congress enacted the *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (PROTECT Act),* which, despite the decision, expanded the definition of "child pornography" to include digital and computer-generated images that are "indistinguishable" from depictions of actual minors engaged in sexually explicit conduct.[14] The Act also established a new pandering provision prohibiting the advertisement, promotion, presentation, or distribution of CSAM, including material that does not constitute "child pornography" but is promoted as such.[15] In *United States v. Williams*, the Supreme Court, without addressing the new definitional language, upheld the constitutionality of the pandering provision, finding the regulation permissible because it targeted the intent to promote illegal CSAM rather than the content of the images themselves.[16] This distinction is important because it underscores the Court's recognition of the broader market for CSAM and the *indirect* harm it

[12] Id at 242.

[13] *See, e.g.,* Doe v. Boland, 698 F.3d 877, 883 (6th Cir. 2012) (holding that laws criminalizing morphed CSAM are constitutional because such material threatens the interests of specific children and there is *de minimis* value to the content); United States v. Hotaling, 634 F.3d 725, 729-30 (2d Cir. 2011) (holding that the First Amendment does not apply to morphed CSAM because such material necessarily harms the reputation and wellbeing of a child); United States v. Mecham, 950 F.3d 257, 265 (5th Cir. 2020) cert. denied, 141 S. Ct. 139 (2020); Shoemaker v. Taylor, 730 F.3d 778, 786 (9th Cir. 2013) ("[M]orphed images are like traditional child pornography in that they are records of the harmful sexual exploitation of children. The children, who are identifiable in the images, are violated by being falsely portrayed as engaging in sexual activity. As with traditional child pornography, the children are sexually exploited and psychologically harmed by the existence of the images, and subject to additional reputational harm as the images are circulated."); *see also,* U.S. v. Salcido, 506 F.3d 729, 733-34 (9th Cir. 2007) (collecting cases from the Second, Fifth, Sixth, Eighth, and Tenth Circuits). The Eighth Circuit is the only exception, holding that the First Amendment protects possession of morphed images that are produced without the hands-on abuse of an actual child is the only exception. *See* United States v. Anderson, 759 F.3d 891, 895 (8th Cir. 2014) (rejecting the argument that morphed images' harms are "indirect harms" like in Ashcroft).

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

[15] S.151, Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003, 108th Leg. Sess., 117 STAT. 650, P.L. 108–21 (Apr. 30, 2003) (proscribing any material that reflects the belief, or that is intended to cause another to believe, that the material is, or contains, an obscene visual depiction of a minor engaging in sexually explicit conduct or is a visual depiction of an actual minor engaging in sexually explicit conduct).

[16] 553 U.S. 285, 291 (2008); *see also* Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 498 (1949) (explaining that the First Amendment affords no protection to speech "used as an integral part of conduct in violation of a valid criminal statute.").

creates. Despite this acknowledgment, the Court reaffirmed the legality of the market for "simulated" CSAM, "so long as it is offered and sought as such, and not as real child pornography."[17]

Since 2008, when the Supreme Court last examined the constitutionality of virtual CSAM, technology has evolved significantly, and the public has a greater understanding of its dangers. Indeed, recent developments, including prosecutions of individuals for the creation and distribution of morphed or virtual images, suggest that law enforcement and courts are increasingly treating AI-generated CSAM as a serious threat.[18] Recently, the U.S. Department of Justice made its first known arrest of a Wisconsin man for the creation, distribution, and possession of wholly synthetic AI-generated CSAM.[19] Though the case is ongoing, it marks a significant first step toward establishing a clear precedent for how AI-generated CSAM is handled under federal law.

i. 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: 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—which includes computer-generated images that are "virtually

[17] Id (arguing that virtual CSAM "do[es] not involve, let alone harm, any children in the production process" and is "not intrinsically related to the sexual abuse of children" and thus "records no crime[,] and creates no victims by its production.").
[18] *See* United States Attorney's Office, Western District of North Carolina, 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 (Nov. 8, 2023), https://www.justice.gov/usao-wdnc/pr/charlotte-child-psychiatrist-sentenced-40-years-prison-sexual-exploitation-minor-and (highlighting the conviction of a child psychiatrist in Charlotte North Carolina for producing, transporting, and possessing CSAM created via a web-based AI application by altering images of clothed minors); U.S. Dep't of Just., Recidivist Sex Offender Sentenced for Possessing Deepfake Child Sexual Abuse Material (May 1, 2024), https://www.justice.gov/opa/pr/recidivist-sex-offender-sentenced-possessing-deepfake-child-sexual-abuse-material (highlighting the conviction of a Pennsylvania man for accessing and possessing images that digitally superimposed the faces of child actors onto the nude bodies of adults engaged in sex acts).
[19] *See* U.S. Dep't of Just., Man Arrested for Producing, Distributing, and Possessing AI-Generated Images of Minors Engaged in Sexually Explicit Conduct (May 20, 2024), https://www.justice.gov/opa/pr/man-arrested-producing-distributing-and-possessing-ai-generated-images-minors-engaged.

indistinguishable" from that of an actual minor, as well as images that have been "created, adapted, or modified," but that appear to depict an "identifiable minor."[20] While this definition seems broad enough to cover AI-generated CSAM, the absence of an actual minor raises questions about whether the content qualifies as "child pornography."

By comparison, 18 U.S.C. §1466A makes it illegal for any person to knowingly produce, distribute, receive, or possess with intent to distribute any visual representation that appears to depict a minor engaging in sexually explicit conduct and is obscene, as well as that which is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse where such representation lacks serious literary, artistic, political, or scientific value.[21] As in § 2252A, computer-generated images are included within the definition of "visual depiction" under § 1466A, but unlike in § 2252A, this statute expressly does not require "that the minor depicted exist."[22] As a result, courts have refused to extend the free speech protections recognized in *Ashcroft* under § 2252A to virtual images proscribed under §1466A.

Violations of § 2252A can result in severe penalties, including up to 10 years imprisonment for possession and 20 years imprisonment for the production and distribution of CSAM.[23] First-time offenders convicted under §1466A face a minimum of 5 years imprisonment and a maximum of 20 years imprisonment.[24] Repeat offenders are subject to harsher penalties under both statutes.[25] Furthermore, 18 U.S.C. §2259 requires defendants convicted under §2252A(9), relating to trafficking in CSAM, to pay restitution to victims in the total amount of losses incurred or reasonably projected to be incurred due to the continued circulation of their images online.[26]

In addition to criminal penalties, 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,

[20] 18 U.S.C. §§ 2256(8)(A)-(C) (excluding "drawings, cartoons, sculptures, or paintings" from "indistinguishable" definition), 2256(9) (defining identifiable minor) 2256(11) (defining the term "indistinguishable" as used with respect to a visual depiction).
[21] 18 U.S.C. §1466A(a)-(c). Although the law does not criminalize the private possession of obscene matter, the act of receiving such matter could violate the statutes prohibiting the use of the U.S. Mails, common carriers, or interactive computer services for the purpose of transportation. *see* § 1466A(d); *see also* 18 U.S.C. § 1460; 18 U.S.C. § 1461; 18 U.S.C. § 1462; 18 U.S.C. § 1463.
[22] 18 U.S.C. §§ 1466A(c), 1466(f)(1).
[23] 18 U.S.C. §2252A(b)(1), (a)(5).
[24] 18 U.S.C. §1466A (a)(2)(b).
[25] Id. *see also* 18 U.S.C. §2252A(b)(1), (a)(5).
[26] §252A(g) (applying in cases in which the series of felony violations involves at least 1 of the violations listed in the subsection).

preliminary, or permanent injunctive relief and to seek compensatory and punitive damages as well as attorneys' fees.[27] 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.[28] Masha's Law provides CSAM victims the right to sue not only those who initially produced the abusive material but also those who perpetuate the exploitation by distributing their imagery, even if there was no actual criminal conviction for the underlying acts.[29] Victims are entitled to $150,000 in liquidated damages per statutory violation, regardless of actual harm suffered, and can also seek compensatory and punitive damages as well as attorney's fees.[30]

ii. The State Statutory Framework

Given the ubiquitous role that the internet plays in facilitating CSAM offenses, federal jurisdiction applies in nearly all cases.[31] Still, offenders can be prosecuted under state "child pornography" and "obscenity" laws in addition to, or instead of, federal law.[32] Indeed, states have a strong interest in crafting their own legal frameworks to address CSAM to ensure that offenders whose actions fall outside federal jurisdiction can be brought to justice.

To that end, at least 39 states and 1 U.S. territory have "child pornography" statutes broad enough to potentially cover AI-generated CSAM.[33] Of those states, 15 explicitly prohibit morphed images

[27] 18 U.S.C. §2252A(f)(1)-(2).
[28] Importantly, § 1466A is not one of the predicate offenses covered under Masha's Law.
[29] 18 U.S.C. §2255(a).
[30] Id.
[31] Federal jurisdiction attaches if CSAM activity occurs in interstate or foreign commerce. 18 U.S.C. §§ 2251, 2252, 2252A. United States law considers the internet an "instrumentality of interstate commerce" to which federal jurisdiction applies. 18 U.S.C. §10.
[32] *See* Citizen's Guide to U.S. Federal Law on Child Pornography, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography (last updated May 28, 2020)
[33] 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. *See* AL ST § 13A-12-194 (providing that the State shall not be required to establish the actual existence or identity of the individual alleged to be under 18 years of age who is engaged in sexually explicit conduct); AK STAT. § 11.61.127 (a) (covering materials involving the use of actual minors engaged in sexual conduct, images that have been manipulated, created, or modified to depict an actual minor engaged in such conduct, and materials that appear to include a minor engaged in such conduct); AZ STAT § 13-3553 (covering visual depictions of actual minors whether created, adapted, or modified); ; ARK. CODE ANN. § 5-27-602 (a)(1) (covering computer-generated reproductions or reconstructions depicting a minor engaged in sexually explicit conduct); CA PENAL § 311.11(covering "other pictorial representations"); CT ST § 53a–193 (covering "computer-generated image or picture, whether made or produced by electronic, digital, mechanical, or other means."); DEL. CODE ANN. tit. 11, §§ 1100, 1109 (covering visual depictions that have been modified to make it appear that a child is engaging in or simulating

sexual conduct and defining child to include any individual who is intended by the defendant to appear to be 14 years of age or less); FL STAT § 847.0135 (c) (covering "any image that has been created, altered, adapted, or modified by electronic, mechanical, or other computer-generated means .to portray a fictitious person, who a reasonable person would regard as being a real person younger than 18 years of age, engaged in sexual conduct."); GA. CODE ANN. § 16-12-100.2(b.2)(providing that it is not a valid defense in a prosecution under this Code section that prior to or while in the control of the accused that the visual medium was created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct); HAW. REV. STAT. § 707- 750 (covering computer-generated images, as well as images created, adapted, or modified to appear that an identifiable minor is engaging in sexual conduct); ID STAT. § 18-1507 (same); 720 ILL. COMP. STAT. 5/11-20.1(4);(f)(7) (2024) (covering computer-generated visual depiction that is, or appears to be, either in whole or in part, a minor); IND. CODE. § 35-42-4-4(d) (providing that it is not a required element of an offense under this Code section that the child depicted actually exists); IA ST § 728.12 ("[A]ny visual depiction that has been created, adapted, or modified to give the appearance that an identifiable minor is engaged in a prohibited sexual act or the simulation of a prohibited sexual act."); KRS STAT. § 21-5510 (covering computer-generated imagery that visually depicts minors); KY STAT. §531.010 (covering computer-generated images, as well as images created, adapted, or modified to appear to be an identifiable minor); MD. CODE §§ 11-207, 208 (covering any matter that depicts a minor engaged as a subject in sexual conduct, or in a manner that reflects the belief, or that is intended to cause another to believe that the minor engaged in such conduct); MICH. COMP. LAWS § 750.145c(b) (covering any depiction that appears to include, or conveys the impression that it includes, a minor if the depiction and was either created using any part of an actual minor or is otherwise obscene); MINN. STAT. §617.246(f)(2)(i)-(iii) (covering any visual depiction, including a computer-generated image, that has been created, adapted, or modified to appear that an identifiable minor is engaging in sexual conduct or that gives the impression that the material is or contains a depiction of a minor engaging in such conduct); MS STAT. §97-5-31 (covering computer-generated images as well as images created, adapted, or modified to appear that an identifiable minor is engaging in sexual conduct); MO. REV. STAT. § 573.01(4)(b)(c) (covering a computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct or that has been created, adapted, or modified to show an identifiable minor engaging in such conduct);MT ST 45-5-625("[A]ny film, photograph, videotape, negative, slide, or photographic reproduction that contains or incorporates in any manner any film, photograph, videotape, negative, or slide.");NE STAT. §28-1463.02(6) (covering photographic representations, including images made or produced by computer, of sexually explicit conduct involving minors); NH REV. STAT. §649-A-2(I), (IV), (V) (effective Jan. 1, 2025) (covering a computer-generated image that is, or is indistinguishable from, that of a child engaging in sexually explicit conduct as well as images that have been created, adapted, or modified to appear that an identifiable minor is engaging in such conduct); NJ REV. STAT. § 2C:24-4 (covering computer-generated images of minors engaged in or simulating a prohibited sexual act); NM STAT. § 30-6A-2 (same); NY PENAL CODE § 245.15 (covering images created or altered by digitization where a person with one or more intimate parts exposed or engaging in sexual conduct may reasonably be identified); NC STAT ANN. § 14-202.7 ("A photograph, film, videotape, recording, live transmission, digital or computer-generated visual depiction, including a realistic visual depiction created, adapted, or modified by technological means, including algorithms or artificial intelligence, such that a reasonable person would believe the image depicts an identifiable individual, or any other reproduction that is created, adapted, or modified by electronic, mechanical, or other means."); OR ST §§163.686,163.687 (covering computer-generated images…whether made or produced by electronic, mechanical or other means); R.I. GEN. LAWS § 11-9-1.3(c)(1)(i)-(iii) (covering a visual depiction, including a computer-generated image, that has been created, adapted, or modified to depict an identifiable minor engaging in sexually explicit conduct); SC STAT. § 16-15-375 (covering "visual depictions or representations but not material consisting entirely of written words."); SD STAT. § 22-24A-2(5), (8) (covering computer-generated images created, adapted, or modified by artificial intelligence that are, or are virtually indistinguishable from, that of an actual child engaging in a sexual act); TN STAT. § 39-17-1002(2)(E) (covering computer-generated images created, adapted, or modified by artificial intelligence that includes a minor engaged in sexual activity); TX PENAL CODE § 43.261(b-1) (covering computer-generated visual material that depicts a recognizable person or that was created, adapted, or modified using artificial intelligence); UT STAT. § 76-5b-103(1)(b)(ii), (c), (3)(a)(ii), (b) (covering artificially generated images that depict an individual with substantial characteristics of a minor engaging in sexually explicit conduct or that have been created, adapted, or modified to appear that an identifiable minor is engaging in such conduct); VA. CODE ANN. § 18.2-374.1(A) (covering sexually explicit images that have been created, adapted, or modified to depict an identifiable minor as well as obscene depictions of minors, whether they exist or not, in a state of nudity or engaged in sexual conduct); WA STAT. 9.68A.011 (covering fabricated images, including those created or altered by using artificial

and synthetic CSAM, provided the content is sufficiently realistic.[34] In some jurisdictions, like California, Idaho, Michigan, and New Mexico, the material must meet the legal standard for obscenity to be prosecuted. Indiana does not explicitly address AI-generated content in its statute, but case law confirms it falls within the state's "child pornography" framework.[35] Another 14 states and 1 U.S. territory expressly prohibit morphed images involving actual children, though

intelligence, that depict an identifiable minor in a realistic manner engaging in sexually explicit conduct); WI STAT. 948.125(1)(a) (covering computer-generated, obscene images of what appears to depict an actual child engaged in sexually explicit conduct but where such child may or may not exist); WYO. STAT. ANN. § 6-4-303(a)(ii)(B) (covering computer-generated images of explicit sexual conduct involving a child or an individual virtually indistinguishable from a child); 14 V.I.C. §489 (covering images created, adapted, or modified to depict an identifiable minor engaging in sexually explicit conduct).

[34] These states are Alabama, Alaska, Delaware, Florida, Idaho, Illinois, Kentucky, Michigan, Montana, Missouri, New Hampshire, North Carolina, South Dakota, Tennessee, and Virginia. *see* AL ST § 13A-12-194; AK STAT. §11.61.127; DEL. CODE ANN. tit. 11, §§ 1100, 1109 ("For the purposes of §§ 1108, 1109, 1110, and 1111 of this title, "child" shall also mean any individual who is intended by the defendant to appear to be 14 years of age or less."); FL STAT. § 827.072; ID STAT. § 18-1507C ("It shall not be a required element of a violation of subsection (1) of this section that the child depicted actually exists."); 720 IL. COMP. STAT. 5/11-20.4 (""Purported child" means a visual representation that appears to depict a child under the age of 18 but may or may not depict an actual child under the age of 18."); KY STAT. 531.010 ("In any prosecution under KRS 531.300 to 531.370 where the offense involves matter or material portraying a computer-generated image of a minor, the Commonwealth shall not be required to prove the actual identity or age of the minor, or that the minor actually exists."); MICH. COMP. LAWS § 750.145c; *see also* People v. Riggs, 604 N.W.2d 68, 237 Mich. App. 584 (1999) (confirming that the statute prohibits the making of a visual image that is a likeness or representation of a child engaging in one of the listed sexual acts.); MN ST § 617.247 ("… advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexual conduct."); MO. REV. STAT. § 573.010 ("Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual minor engaged in sexually explicit conduct"); representations, including images made or produced by computer, of sexually explicit conduct involving minors); NH REV. STAT. §649-A-2(effective Jan. 1, 2025) ("Indistinguishable means virtually indistinguishable, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual child engaged in sexually explicit conduct. This definition does not apply to depictions that are drawings, cartoons, sculptures, or paintings depicting minors or adults."); NC STAT. ANN. § 14–202.7; SD STAT. § 22-24A-2 ("An individual indistinguishable from an actual minor created by the use of artificial intelligence or other computer technology capable of processing and interpreting specific data inputs to create a visual depiction."); TN STAT. § 39-17-1002 ("Generative artificial intelligence" means an artificial intelligence system that is capable of creating new content or data, including text, images, audio, or video, when prompted by an individual.); VA. CODE ANN. § 18.2-374.1 ("…the minor depicted does not have to actually exist.").

[35] *See* infra n. 32; *see also* Logan v. State, 836 N.E.2d 467 (2005) (As written, the statute prohibiting child pornography was overbroad, but not substantially so, and the mere fact that statute exceeded the permissible bounds of what the legislature might regulate did not necessarily lead to the conclusion that the statute was constitutionally infirm pursuant to First Amendment's overbreadth doctrine; on its face, statute applied to not only visual child pornography, but also written descriptions of child pornography, and statute applied to written descriptions of child pornography, virtual child pornography, and pornography showing youthful-looking adults.)

they stop short of regulating entirely synthetic content.[36] Meanwhile, 13 states and 4 U.S. territories do not appear to criminalize AI-generated CSAM at all.[37]

Even among states with statutes broad enough to potentially cover AI-generated CSAM, there is significant variability in terms of their scope and outcome. For example, 32 states penalize private possession of CSAM.[38] Some, like New Hampshire and Nebraska, restrict prosecution to possession with intent to sell, while Alabama and the U.S. Virgin Islands limit it to possession with intent to distribute. In Kansas and South Carolina, the prosecution must prove possession for a sexual purpose.[39] Thirty states and 1 U.S. territory criminalize the distribution, dissemination, or publication of AI-generated CSAM, though in Kentucky and Mississippi, there must be intent to sell or profit.[40] At least 25 states and 1 U.S. territory prohibit the creation or production of AI-generated CSAM, with North Carolina only prosecuting production for pecuniary gain.[41] Some states, such as Alaska, Florida, and Texas, criminalize accessing or viewing AI-generated CSAM alone, without intent to distribute.[42]

The vast majority of states with broadly written statutes explicitly reference "computer-generated images"[43] or adopt inclusive terms like "any material" or "any representation" to cover a range of

[36] 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* infra n.34.
[37] 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* infra n. 34.
[38] These states are Alaska, Arkansas, Arizona, California, Connecticut, Delaware, Georgia, Florida, Hawaii, Idaho, Iowa, Illinois, Indiana, Kentucky, Maryland, Michigan, Montana, Mississippi, Minnesota, Missouri, New Jersey, New Mexico, North Carolina, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin, and Wyoming. *see* infra n.34.
[39] In Kansas, the possession must be with intent to arouse or satisfy the sexual desires of the offender or another person. KS ST 21-5510. In South Carolina, possession is proscribed "if a reasonable person would infer the purpose is sexual stimulation." SC STAT. §§ 16-15-405, 16-15-395
[40] 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* infra n. 34.
[41] 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. *See* infra n. 32.
[42] Alaska prohibits accessing with intent to view; Arkansas and Florida prohibit intentional viewing; Idaho prohibits accessing; Indiana and Oregon prohibit accessing with an intent to view; Michigan prohibits seeking and accessing; and New Jersey and Texas prohibit viewing. *See* infra n. 34.
[43] These jurisdictions include Alabama, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Kansas, Kentucky, Maryland, Michigan, Minnesota, Mississippi, Missouri, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Oregon, Rhode Island, Utah, Wisconsin, and Wyoming. *See* infra n. 34.

exploitative content.[44] Some 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.

"Sexual conduct," in turn, is defined by most states to include sexual, oral or anal intercourse, bestiality, masturbation, sado-masochistic abuse, and lascivious exhibition of the genitals.[45] Interpretations of "lascivious exhibition" vary widely across jurisdictions. Many states require that the exhibition be intended to appeal to "prurient interests" or offend community standards, while others assess the context of the image—analyzing factors such as setting, posture, or the actions depicted. Texas, Virginia, and Washington, D.C., for example, emphasize context, recognizing that even partial nudity can be considered lascivious if presented in a sexualized manner. By contrast, Arkansas and the U.S. Virgin Islands focus more on the creator's intent, permitting prosecution of sexually suggestive, though non-explicit, content. Many courts apply the *Dost* test to determine if a given image is "lascivious" under the law.[46] The test requires a case-by-case analysis of the following six-factors: (1) whether the genitals or pubic area are the focal point of the image; (2) whether the setting of the image is sexually suggestive (i.e., a location generally associated with sexual activity, such as a bed); (3) whether the subject is depicted in an unnatural pose or inappropriate attire considering their age; (4)whether the subject is fully or partially clothed, or nude; (5)whether the image suggests sexual coyness or willingness to engage in sexual activity; and (6)whether the image is intended or designed to elicit a sexual response in the viewer.[47]

Beyond "child pornography" laws, all 50 states and 6 U.S. territories maintain obscenity statutes. Most state laws were originally crafted to protect minors from accessing and viewing sexually explicit materials or to regulate obscene content more broadly. As a result, many of these statutes

[44] *See, e.g.,* Arkansas (any reproduction or reconstruction); Iowa (any visual depiction); South Carolina (other visual depictions or representations); Texas (any photographic reproduction). *See* infra n. 34.
[45] *See, e.g.,* Alabama, Delaware, Minnesota, and New Mexico. *See* infra n. 34.
[46] *See* United States v. Dost, 636 F. Supp. 828, 832 (S.D. Cal. 1986), aff'd sub nom., United States v. Wiegand, 812 F.2d 1239, 1244 (9th Cir. 1987).
[47] Id.; *see, e.g.,* , United States v. Arvin, 900 F.2d 1385 (9th Cir. 1990) (permitting jurors to consider the caption on a photograph); United States v. Villard, 885 F.2d 117, 124 (3d Cir. 1989) ("[A] photograph of a naked girl might not be lascivious (depending on the balance of the remaining Dost factors), but a photograph of a girl in a highly sexual pose dressed in hose, garters, and a bra would certainly be found to be lascivious.")

focus on the sale, distribution, and exhibition of traditional media—such as books, films, and videos—that involve a direct link to physical human actors.[48] Most state obscenity statutes do not explicitly include computer-generated content, though some use catch-all terms like "visual representations," "pictorial representations," or "other representations" that could potentially cover AI-generated images.[49] State laws, many of which rely on archaic definitions of obscene content, are ill-suited for addressing the unique threats posed by modern digital technologies. With that understanding, a handful of states have proactively updated their laws to reflect the modern digital landscape. For example, California recently passed legislation that explicitly bans "obscene visual representations of the sexual abuse of children," including AI-generated images.[50] This law establishes clear accountability for those using AI to create, distribute, or possess obscene material, setting a precedent for other states to follow.

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.[51] States

[48] *See, e.g.*, HI REV. STAT. § 712-1210; MD CODE § 11-203; MN STAT. ANN. § 617.293.
[49] *See, e.g.*, IN CODE § 35-49-1-3(2) (Indiana); 720 ILCS 5/11-20 (Illinois); NE REV. STAT. § 28-807(7); TN CODE ANN. § 39-17-901(7) (Tennessee).
[50] AB 1831, 2023-2024 Leg. Sess. (Sep. 29, 2024).
[51] 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. AL ST §13A-6-240 (providing for recovery of the full actual damages incurred, punitive damages, and attorney's fees); AK STAT. § 09.55.650 (providing that any person who, as a minor under age 16, was the victim of child pornography may bring an action for recovery of damages against the perpetrator based on the perpetrator's intentional conduct for an injury or condition suffered as a result of the offense), FLA. STAT. § 847.01357 (providing a civil cause of action for any person who, while a minor, was a victim of child pornography and suffered personal or psychological injury as a result against the perpetrator); KAN. STAT. ANN. § 60-5001 (providing a civil cause of action for any person who, while a minor, was a victim of child pornography, where such offense resulted in a conviction and any portion of such offense was used in the production of child pornography, and who suffers personal or psychological injury as a result of the production, promotion, or possession of such child pornography and stating that an action may be brought against the producer, promoter or intentional possessor of such child pornography); MASS. GEN. LAWS ch. 265, § 50 (providing that a victim subjected to the production of unlawful pornography may bring an action in tort); MINN. STAT. § 617.245 (Subd. 2) (providing for a cause action for injury caused by the use of a minor in a sexual performance which may be brought against a person who promotes, employs, uses, or permits a minor to engage or assist others in engaging in a sexual performance); MO. REV. STAT. § 537.047 (providing for a cause of action for any person who, while a minor, was a victim of CSAM and suffered physical or psychological injury or illness as a result); MT. CODE ANN. § 27-2-216 (providing that a victim of child pornography may bring a tort action for recovery of damages for injury suffered as a result); NEB. REV. STAT. § 25-21,292 (providing a civil cause of action for "any participant or portrayed observer in a visual depiction of sexually explicit conduct" who suffered personal or psychological injury which may be brought against any person who knowingly and willfully created, distributed, or actively acquired such visual depiction, or aided or assisted with the same, while in the state); N.H. REV. STAT. ANN. § 633:11 (providing that a victim who was compelled to perform a "sexually-explicit performance," which includes photographs or videotapes "involving one or more sex acts," may bring a civil action against a person that commits the offense for damages, injunctive relief, or other appropriate relief); N.J. STAT. ANN. § 2A:30B-3 (providing that "[a] child can bring a civil

such as Florida, Kansas, and Oklahoma allow the victim of a CSAM crime that resulted in a personal or psychological injury to bring a civil action against their perpetrator.[52] Successful plaintiffs in these states are entitled to recover actual damages as well as court costs and attorney fees.[53] In Oklahoma, the law also allows for the recovery of special and punitive damages, [54] while in Florida and Kansas, victims are guaranteed a minimum of $150,000 in damages for each violation.[55]

South Dakota similarly allows victims to bring civil claims against individuals convicted of CSAM crimes, with potential compensation that includes both economic and non-economic damages, as well as exemplary damages, attorney's fees, and court costs. [56] In New Jersey, victims are entitled to recover triple the amount of damages based on the financial gains the defendant derived from the illegal activity, along with full legal costs and attorney's fees.[57]

In several other states—including Florida, Connecticut, New Mexico, Louisiana, Texas, and Wisconsin—the government provides victims with compensation for mental health services such

against a person who commits one or more of a variety of child pornography acts); N.C. GEN. STAT. § 14–190.5A(g) (effective Dec. 1, 2024) (providing a civil cause of action based on the disclosure of private images for any person whose image is disclosed, or used, as described by the offense, against any person who discloses or uses the image); OKLA. STAT. tit. 21, § 1040.56 (providing a civil cause of action for any person who, while a minor, was a victim of child pornography and suffered personal or psychological injury as a result which may be brough against the perpetrator); 18 PA. CONS. STAT. § 3051 (providing a civil cause of action for a victim of child pornography which may be brought against a participant of the crime); R.I. GEN. LAWS § 9-1-2 ("Whenever any person shall suffer any injury to his or her person, reputation, or estate by reason of the commission of any crime or offense, he or she may recover his or her damages for the injury in a civil action against the offender."); S.D. CODIFIED LAWS §§ 22-24A-7, 22-24A-10 (providing a civil cause of action for damages against a person who commits a child pornography crime); UTAH CODE ANN. § 77-38-15 (providing a civil cause of action for victims of human trafficking, including forced participation in the production of pornography, against the perpetrator or anyone who knowingly benefitted from the trafficking); VA. CODE ANN. § 8.01-42.4 (providing for a civil cause of action for victims of trafficking that includes victims of a manufacturer of child pornography); WASH. REV. CODE § 9.68A.130 (providing that a minor prevailing in a civil action arising from the sexual exploitation of a child is entitled to recover the costs of the suit, including an award of reasonable attorney's fees.); WIS. STAT. § 948.051 (providing for a civil cause of action for any person who suffers an injury or death as a result of child trafficking, which includes certain child pornography offenses, which may be brought against the person who committed the violation.); NMI 3116 (providing a civil cause of action against violators for compensatory damages and injunctive relief).

[52] FL STAT. § 960.197; KAN. STAT. ANN. § 60-5001; OK STAT. T. 21, § 1040.56.

[53] ID.

[54] OK STAT. T. 21, § 1040.56.

[55] FL STAT. § 960.197; KAN. STAT. ANN. § 60-5001

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

[57] N.J. STAT. ANN. § 2A:30B-3(a).

as counseling to address psychological trauma caused by the crime.[58] This compensation is not dependent on the successful criminal prosecution of the offender.

States such as Arizona, Idaho, Kentucky, New Jersey, Oregon, Pennsylvania, South Carolina, Tennessee, Utah, Vermont, Virginia, and West Virginia also have similar programs to assist victims who have suffered emotional or physical harm due to a crime. [59] In New Hampshire and Washington, these programs extend only to victims of crimes classified as felonies. [60]

iii. Regulatory Framework for Developers and Online Service Providers

As part of a national effort 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, among other things, 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.[61] On May 7, 2024, President Biden signed the *Revising Existing Procedures on Reporting via Technology (REPORT) Act* into law, which expands these reporting obligations.[62] While previous reporting requirements under §2258A only addressed the presence of known CSAM, the Act mandates that internet service providers report not only existing CSAM but also "planned," "imminent," and "apparent" violations of federal CSAM laws occurring on their platforms.[63] Additionally, the Act increases the statutory penalties for knowing and willful failures to report online sexual exploitation of children from $150 -$300 thousand to $600 thousand-$1 million, depending on the provider's size.[64] Notably, these reporting obligations only apply to violations under §2252A, not §1466A, meaning providers are not required to report obscene content, such as AI-generated cartoons, that do not depict the abuse of actual minors.[65] As AI-generated content becomes increasingly realistic, these materials are more

[58] 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.*
[59] 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.
[60] N.H. REV. STAT. ANN. § 21-M:8-h; WASH. REV. CODE § 7.68.020.
[61] PROTECT Our Children Act of 2008, Pub. L. 110-401, Oct. 13, 2008, 122 Stat. 4229 (18 U.S.C. 2258A to 2258E; 34 U.S.C. 21101 et seq.)
[62] REPORT Act of 2023, Pub. L. 118–59, §§ 3, 4(a), May 7, 2024, 138 Stat. 1016.
[63] Id.
[64] Id.
[65] *See* 18 U.S.C. §2258A (a)(2)(A).

likely to be flagged under §2252A, placing further strain on the already overwhelmed reporting system.

The emergence of AI technologies also presents complex legal questions regarding whether companies that develop or deploy these tools can be held liable for illegal or harmful content their systems generate. Central to the issue is §230 of the *Communications Act of 1934*, enacted as part of the *Communications Decency Act (CDA) of 1996*, which grants online service providers a limited defense from liability for third-party content hosted on their platforms.[66] Specifically, §230(c)(1) protects providers and users of an "interactive computer service" from being treated as publishers or speakers of user-generated content, while §230(c)(2) grants immunity for good-faith efforts to restrict user access to offensive or indecent material. "Interactive computer service" is broadly defined to include "any information service, system, or access software provider" that offers tools to "filter, screen, allow, or disallow content," "pick, choose, analyze, or digest content," or "transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content"—functions that align with the operations of many generative AI systems.[67]

Over time, federal courts have transformed §230's limited defense into a *de facto* immunity shield from liability for not only "publisher" claims but "distributor" claims as well.[68] This broad interpretation has enabled online service providers to evade accountability for a variety of illicit activities on their platforms, including child sex trafficking.[69] In response, Congress passed the *Fight Online Trafficking Act* and the *Stop Enabling Sex Traffickers Act (FOSTA-SESTA)* in 2018, which clarified that §230 immunity does not extend to sex traffickers or those that profit from sex trafficking, including online service providers who know or should know that their platforms are being used for trafficking in CSAM.[70] Courts also have limited immunity in cases where platforms

[66] 47 U.S.C. § 230.
[67] 47 U.S.C. § 230(f)(2), (4); *see also* Ricci v. Teamsters Union Local 456, 781 F.3d 25, 27–28 (2d Cir. 2015) (observing that the definition of interactive computer service "has been construed broadly to effectuate the statute's speech-protective purpose").
[68] *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 331-33 (4th Cir. 1997).
[69] *See, e.g.*, Doe v. Backpage.com, LLC, 817 F.3d 12, 18–24 (1st Cir. 2016) (applying Section 230(c)(1) to claims brought under federal and state sex trafficking statutes); Doe v. MySpace, Inc., 528 F.3d 413, 420 (5th Cir. 2008) (rejecting negligence liability for a service provider when an adult user used the service to meet and allegedly abuse minor children).
[70] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 1115-164, 132 Stat. 1253 (2018); *see also* Doe #1 v. MG Freesites, Ltd., 2022 WL 407147, at *12 *N.D. Ala. Feb. 9, 2022) (noting that 18 U.S.C. § 1595(a) allows "sex trafficking victims to bring civil claims against 'whoever knowingly benefits, financially or by receiving anything of value from participation in a venture which that person knew or should have known has engaged

act as "information content providers" by contributing "in whole or in part" to the creation or development of unlawful content.[71]

In *Fair Housing Council of San Francisco Valley v. Roommates.com LLC*, the Ninth Circuit introduced the "material contribution" test to determine when an online service provider operates beyond the protections of §230.[72] The court distinguished between neutral tools—such as a blank text box where users input information—and systems that, by design, require discriminatory inputs, such as drop-down menus limiting housing listings based on protected characteristics.[73] The Court determined that platforms that act merely as intermediaries retain immunity, but those that design or solicit content are deemed co-creators and lose §230 protection.[74]

Courts have not yet decided whether or how §230 may be used as a defense 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 that was generated entirely by the platform itself.[75] 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 similar name.[76] Although §230 has not been used as a defense in either case, courts may soon need to decide whether generative AI outputs are considered third-party or original content.

Unfortunately, the near absolute immunity granted to online service providers under §230 has limited incentives to proactively combat the spread of CSAM on their platforms, prompting Congress to introduce legislation to address the issue. For example, 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

---

in an act in violation of this chapter.'"); Does #1-6 v. Reddit, Inc., 51 F4th 1137, 1140-41 (9th Cir. 2022), cert. denied sub nom., 143 S. Ct. 2560 (U.S. 2023); Doe v. Mindgeek USA, Inc., 558 F. Supp. 828, 835 (C.D. Cal. 2021).

[71] *See, e.g.*, FTC v. Accusearch Inc., et al, No. 08-8003 (10th Cir. 2009).

[72] 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc) (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").

[73] Id.

[74] Id.

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

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

laws.[77] 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. [78] Another proposal, the *Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment (STOP CSAM) Act*, expands reporting requirements for online service providers and creates a new cause of action for victims to sue them over CSAM-related harm.[79] 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)*[80] and the *Kids Online Safety Act (KOSA)* [81]—are advancing through Congress, both of which target children's online privacy and safety concerns. COPPA 2.0 would ban targeted advertising to users under 17, establish a mechanism for deleting personal data, and create a new *Youth Marketing and Privacy Division* within the Federal Trade Commission.[82] KOSA would require digital platforms to adopt safety-by-design, protect minors' personal information, disable addictive features, and allow users to opt out of algorithmic recommendations.[83] Together, these reforms signal a growing effort to hold platforms accountable for harm to children while increasing transparency and privacy protections for young users.

B. NONCONSENSUAL DISTRIBUTION OF INTIMATE IMAGES & UNAUTHORIZED DIGITAL REPLICAS

A variety of laws are available at both the state and federal levels to protect individuals from the unauthorized use of their likeness, including statutes that specifically address the growing threat of so-called "deepfakes."[84] Many states have enacted or are actively considering legislation aimed

[77] S.1207, EARN IT Act of 2023, 118th Cong. Sess. (2023-2024)
[78] Id.
[79] H.R.7949, Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act of 2024, 118th Congress (2023-2024).
[80] S.1418, Children and Teens' Online Privacy Protection Act, 118th Congress (2023-2024).
[81] H.R.7891, Kids Online Safety Act, 118th Congress (2023-2024).
[82] Supra n. 81.
[83] Supra n. 82.
[84] 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.

at addressing unauthorized digital replicas and nonconsensual distribution of intimate images.[85] The primary approach taken in the states involves amending existing "revenge porn" laws to cover deepfake images and videos and introducing new privacy and right of publicity cause of actions. Right of publicity legislation has also been introduced at the federal level, which, if adopted, would create a national standard for prosecuting and addressing nonconsensual AI-generated deepfakes. Federal Copyright and consumer protection laws may also offer victims some protection, but these laws are narrowly applied. Comprehensive federal legislation is urgently needed to address the growing epidemic of image-based abuse and the serious harm it inflicts on those depicted, including children.

i. The Federal Legal and Regulatory Frameworks

1. Non-consensual Distribution of Intimate Images

At the federal level, there is no criminal statute directly targeting the distribution of nonconsensual sexual images.[86] 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 unauthorized distribution of intimate images of both adults and children.[87] The term "intimate visual depiction" under §1309(a)(5) is given the same meaning as that provided for a "visual depiction" under 18 U.S.C. §2256(5), and includes, among other things, material that depicts an "identifiable" individual engaging in "sexually explicit conduct" as defined in 18 U.S.C. §§ 2256(2)(A) and (B). Properly interpreted, §1309 protections would then extend to AI-generated CSAM that incorporates morphed images of actual, identifiable minors, but not to wholly synthetic CSAM. 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

[85] This refers to the distribution of sexual or pornographic images of individuals without their consent. This may include images taken without consent or images taken with consent but later distributed without the consent of those depicted in the images. These images are often referred to as "revenge porn."
[86] 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.
[87] P.L. 117-103 (2022).

images to seek recovery of monetary damages and to enjoin the defendant from further distributing their image.[88] Notably, §1309 is silent about whether or how it might interact with §230.

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)*,[89] the *Nurture Originals, Foster Art, and Keep Entertainment Safe Act of 2024 (NO FAKES)*,[90] and the *Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024 (DEFIANCE)*.[91] These legislative efforts aim to address the exploitation of digital replicas and the psychological, reputational, and privacy harms associated with the nonconsensual disclosure of AI-generated sexual imagery. Together, they reflect a growing recognition of the need to modernize federal law to keep pace with emerging technologies and to ensure victims have robust legal protections.

a) No AI FRAUD Act

Introduced in early 2024, the No AI FRAUD Act provides intellectual property-like protections over one's voice and likeness by prohibiting the unauthorized use of digital replicas.[92] The legislation requires that authorization for the use of a digital depiction or voice replica be provided in writing. This authorization is only valid if legal counsel represents the individual. Minors must also receive court approval for such agreements.[93]

The bill establishes direct liability for individuals or entities that distribute digital voice replicas or depictions with knowledge of their unauthorized nature. It further imposes liability for trafficking in "personalized cloning services" that are specifically designed to create digital replicas of specific individuals. Additionally, the legislation imposes secondary liability on those who, with knowledge of lack of consent, "materially contribute to, direct, or otherwise facilitate" such conduct. To address First Amendment concerns, the bill introduces a balancing test for courts to weigh the public interest against the privacy and personal rights of individuals depicted in digital

[88] 15 U.S.C §6851.
[89] HR 6943, No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act, 118th Congress (2023-2024).
[90] HR 9551, Nurture Originals, Foster Art, and Keep Entertainment Safe Act of 2024, 118th Congress (2023-2024).
[91] S3696, Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024,118th Congress (2023-2024).
[92] Supra n. 90.
[93] Id.

replicas. However, this test is inapplicable when the digital depiction involves CSAM, sexually explicit content, or intimate images.[94]

b) NO FAKES Act

In September 2024, Congress introduced the NO FAKES Act, which seeks to grant all individuals, including children, a federal intellectual property right over their own voice and likeness and to prohibit the creation and distribution of unauthorized digital replicas.[95] If passed, it would create a national standard regarding the use of unauthorized AI-generated content.

Because the bill creates an intellectual property right, individuals and entities, including online service providers, would be liable under §230 for producing, hosting, or distributing unauthorized deepfakes. Hosting platforms would also be obligated to remove infringing replicas upon notice. Violations of the law could result in a plaintiff recovering the greater of either statutory or actual damages, as well as punitive damages, and attorney's fees.[96]

c) DEFIANCE Act

The DEFIANCE Act seeks to expand the protections in §1309 to cover "digital forgeries"—unauthorized, AI-generated depictions of identifiable individuals.[97] The bill, if passed, would allow victims to seek damages from anyone who "knowingly produced or possessed" the AI-generated image with the intent to distribute it where the individual depicted did not consent to the conduct.[98] Purely synthetic depictions that do not involve an actual, identifiable individual are not covered unless they are deemed obscene under a separate statute. Any person aggrieved by a violation of law would be able to seek injunctive relief, punitive damages, and the greater of either $150,000 in liquidated damages or actual damages, and to recover any revenue generated by the defendant as a result of the dissemination of their images.[99]

2. Copyright Law

[94] Id.
[95] Supra n. 91.
[96] Id.
[97] Supra n. 92.
[98] Id.
[99] Id.

Copyright law protects original works of authorship, including photographs, audio recordings, and videos, which may be used to create digital replicas.[100] Under the Copyright Act, copyright owners are granted exclusive rights, such as the right to reproduce their work and create derivative works.[101] Morphed images that incorporate or manipulate preexisting copyrighted material—may infringe upon these exclusive rights. If the individual depicted owns the copyright to the underlying material, they may have grounds for a copyright infringement claim over the entire work. However, copyright law does not protect an individual's identity in and of itself, meaning that a replica of their image or voice alone would not constitute copyright infringement. [102]

This distinction is particularly important in the context of AI-generated CSAM. If AI-generated CSAM includes a copyrighted image of a child—whether produced by a photographer or as self-generated content—the copyright owner could pursue an infringement claim.

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.*, 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.[103] The Court rejected the plaintiff's argument that copyright's adaptability to new technologies is expansive enough to contemplate AI authorship, emphasizing that human authorship—and, more specifically, human creativity—is the "sine qua non at the core of copyrightability."[104] 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.[105]

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

[100] 17 U.S.C § 106.
[101] 17 U.S.C. § 102(b)
[102] Id.
[103] No. 1:2022cv01564 (D.D.C. 2023).
[104] Id at 8.
[105] United States Copyright Office, Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 16190 FEDERAL REGISTER, VOL. 88, NO. 51, 37 CFR PART 202 (Mar. 16, 2023).

model.[106] 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. [107]

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.

3. Consumer Protection Law

The Federal Trade Commission (FTC) plays a critical role in consumer protection by enforcing regulations that prohibit "[u]nfair methods of competition" and "unfair or deceptive" practices "in or affecting commerce." [108] The FTC has affirmed that AI technologies are not exempt from oversight.[109]

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.[110] 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.[111] 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.[112] This provision has significant implications for

[106] Paul Tremblay, et. al. v. OpenAI, Inc, et al., 23-cv-03223-AMO (N.D. Cal. Feb. 12, 2024); The New York Times v. Microsoft Corp., OpenAI, Inc., et al., 1:23-cv-11195, (S.D. NY Dec. 27, 2023).
[107] 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).
[108] 15 U.S. Code § 45(a)(1) ("Federal Trade Commission Act").
[109] *See* Federal Trade Commission, Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems (April 25, 2023), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/joint-statement-enforcement-efforts-against-discrimination-bias-automated-systems.
[110] *See* Federal Trade Commission, FTC Announces Impersonation Rule Goes into Effect Today (April 1, 2024), available at https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-impersonation-rule-goes-effect-today.
[111] Supplemental Notice of Proposed Rulemaking, 89 Fed. Reg. 15072 (proposed Mar. 1, 2024) (to be codified at 16 C.F.R. pt. 461).
[112] Id.

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.

ii. State Legal and Regulatory Frameworks

1. Statutory and Common Law Privacy Torts

Deepfakes violate personal privacy by exploiting an individual's likeness without consent, often resulting in significant emotional, psychological, and reputational harm. When deepfakes involve children—especially through the use of morphed images that insert a child's face into explicit content—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.[113]

At least 9 states and 1 U.S. territory explicitly recognize false light as a distinct privacy tort.[114] 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

[113] The common law right of privacy first emerged in the late 19th century and has since evolved into a widely recognized legal principle, with most states acknowledging some form of the right through statutory or common law. Rather than a singular tort, the right of privacy is often described as a "complex of torts," encompassing four distinct claims: (1) intrusion upon seclusion or solitude, (2) public disclosure of embarrassing private facts, (3) false light, and (4) appropriation of a person's name or likeness. *See generally*, J. THOMAS MCCARTHY & ROGER E. SCHECHTER, THE RIGHTS OF PUBLICITY AND PRIVACY §§ 6:1, 6:7 (2d ed. 2024); RESTATEMENT (SECOND) OF TORTS § 652I (AM. L. INST. 1977); *see also* William L. Prosser, Privacy, 48 CALI. L. REV. 383, 389 (1960) ("It is not one tort, but a complex of four.").

[114] These include Arizona, California, D.C., Georgia; Illinois, Indiana, Michigan, New Jersey, Ohio, and Pennsylvania. Godbehere v. Phoenix Newspapers, Inc., 783 P.2d 781, 787 (1989); Gill v. Curtis Publ'g Co., 239 P.2d 630 (Cal. 1952); Klayman v. Segal, 783 A.2d 607, 613 (D.C. 2002); Association Servs. v. Smith, 549 S.E.2d 454, 459 (Ga. Ct. App. 2001); Lovgren v. Citizens First National Bank, 534 N.E. 2d 987 (1989); St. John v. Town of Ellettsville, 46 F. Supp. 2d 834, 851 (S.D. Ind. 1999); Morganroth v. Whitall, 411 N.W.2d 859, 863-64 (Mich. Ct. App. 1987); Romaine v. Kallinger, 537 A.2d 284, 290 (N.J. 1988); Welling v. Weinfeld, 866 N.E.2d 1051 (Ohio 2007); Curran v. Children's Serv. Ctr. Inc., 578 A.2d 8, 12 (Pa. Super. Ct. 1990).

person," and if "the actor had knowledge of or acted with reckless disregard for the falsity."[115] 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 are enough. Although an emerging remedy for unauthorized and illicit deepfakes, courts have imposed liability where a defendant spread false statements attributing "a lewd fantasy" to a woman and falsely claimed she had agreed to appear in an adult magazine,[116] and where a defendant used an individuals' name and likeness in promotions for strip clubs. [117]

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."[118] Courts have interpreted this tort inconsistently. In several states, the appropriation must be undertaken for a commercial purpose, thereby excluding individuals harmed by other noncommercial uses.[119] In other jurisdictions, the tort is limited to those whose names or likenesses have "intrinsic value," effectively protecting only public figures. [120] Other states do not recognize the tort at all.[121]

2. Right of Publicity

The term "Right of Publicity" was first recognized by the Second Circuit in *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc*., which held that "in addition to and independent of that right of privacy . . . , a man has a right in the publicity value of his photograph, i.e., the right to grant the exclusive privilege of publishing his picture. . . ."[122] This decision marked the transformation of

[115] *See* RESTATEMENT (SECOND) OF TORTS § 652E (AM. L. INST. 1977); *see also* 1 J. THOMAS MCCARTHY & ROGER E. SCHECHTER, THE RIGHTS OF PUBLICITY AND PRIVACY § 5:114 n.1 (2d ed. 2024) ("The courts uniformly adopt the Restatement of Torts list of elements.").
[116] Wood v. Hustler Mag., Inc., 736 F.2d 1084, 1089, 1093 (5th Cir. 1984).
[117] Longoria v. Kodiak Concepts LLC, 527 F. Supp. 3d 1085, 1102 (D. Ariz. 2021).
[118] DAN B. DOBBS, PAUL T. HAYDEN & ELLEN M. BUBLICK, THE LAW OF TORTS § 579 (2d ed. 2024).
[119] *See, e.g.*, MASS. STAT. ANN. Ch. 214, § 3A (providing for a civil cause of action for use of name, portrait, or picture for advertising or trade purposes without written consent); Fergerstrom v. Hawaiian Ocean View Estates, 441 P.2d 141 (Haw. 1968) (holding that a cause of action for the appropriation of another's name or picture applies only to use for commercial purposes in Hawaii).
[120] *See, e.g.,* Cox v. Hatch, 761 P.2d 556 (Utah 1988) (expressly requiring that plaintiffs' identities have some kind of intrinsic value).
[121] *See, e.g.*, Hougum v. Valley Mem'l Homes, 1998 ND 24, ¶ 12, 574 N.W.2d 812, 816 ("This Court has not decided whether a tort action exists in North Dakota for invasion of privacy."); Nelson v. J.C. Penney Co., 75 F.3d 343, 347 (8th Cir. 1996).
[122] 202 F.2d 866, 868 (2d Cir. 1953).

the right of publicity into a fully transferable intellectual property right, that has since been invoked by, among others, Facebook users and victims of revenge porn.[123]

Today, 37 states recognize the right of publicity through statute, common law, or both.[124] Some states—such as Alaska, Kansas, Maryland, and North Carolina—have neither a statutory nor common law right of publicity.[125]

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. In some states the law sweeps broadly, capturing aspects of identity that merely evoke or call to mind the protected individual. For example, the Ninth Circuit held that a robotic depiction of a blonde woman in a long gown turning large block letters on a game-show set sufficiently "evoked" the likeness of Vanna White under California's common law right of publicity, even without using her

[123] *See, e.g.*, Hepp v. Facebook, Inc., 465 F. Supp. 3d 491 (2021).

[124] States that only have a statutory right include: Arkansas, Hawaii, Illinois, Indiana, Louisiana, New York, Rhode Island, South Dakota, Nevada, Nebraska, and Virginia. *See* AR CODE 4-75-1101; HI REV. STAT. § 482P-1 *et seq.*; 765 ILCS 1075/1 *et seq.*; IN CODE § 32-36-1-0.2 *et seq.*; LA REV. STAT. ANN. 14:102.21; N.Y. CRL § 50; R.I. GEN. STAT. § 9-1-28; SD STAT. § 21-64 *et seq.;* NV REV. STAT. ANN. §597.770 *et seq.;* NE REV. STAT. §§ 20-201 et seq. VA CODE §§ 8.01-40, 18.2-216.1. States that only have a common law right include: Connecticut (Jackson v. Roberts, No. 19-480 (2d Cir. Aug. 19, 2020), Colorado (Donchez v. Coors Brewing Co., 392 F.3d 1211 (10th Cir. 2004)), Delaware (Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481 (3d Cir. 1956)); D.C. (Lane v. Random House, Inc., 985 F. Supp. 141 (D. D.C. 1995)), Georgia (Bullard v. MRA Holding, LLC, 740 S.E.2d 622 (Ga. 2013)), Michigan (Rosa and Raymond Parks Institute for Self-Development v. Target Corp., No. 15-10880 (11th Cir., Jan. 4, 2016)), Missouri (Doe v. TCI Cablevision, 110 S.W.3d 363 (Mo. 2003)); New Jersey (Hart v. Elec. Arts. Inc., 717 F.3d 141 (3d Cir. 2013)), New Mexico (Moore v. Sun Pub. Corp., 881 P.2d 735 (N.M. 1994)), New Hampshire (Doe v. Friendfinder Network, Inc., 540 F. Supp 2d 288 (D.N.H. 2008)), South Carolina, (Gignilliat v. Gignilliat, Savitz & Bettis L.P., 684 S.E.2d 756 (S.C. 2009)), Oregon, (Anderson v. Fisher Broad. Co., 712 P.2d 803 (Or. 1986)), and West Virginia, (Curran v. Amazon.com, 86 U.S.P.Q.2d 1784 (S.D. W. Va. 2008)). States that have both a statutory and common law right include: Alabama (AL CODE § 6-5-770 *et seq.*; Allison v. Vintage Sports Plaques, 136 F.3d 1443 (11th Cir. 1998)), Arizona (AZ REV. STAT.. § 12-761; In re Estate of Reynolds, 327 P.3d 213 (Ariz. Ct. App. Div. 1 2014)), California (CAL CIV. CODE § 3344; Comedy III Prods. v. Saderup, 21 P.3d 797 (Cal. 2001)); Florida (FL STAT. §540.08; Weaver v. Myers, 229 So.3d 1118 (Fla. 2017)); Kentucky (KY REV. STAT. § 391.170; W. & S. Fin. Grp. Beneflex Plan, 797 F. Supp. 2d 796 (W.D. Ky. 2011)); Ohio (OH REV. CODE § 2741 et seq; Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977)); Oklahoma (OK STAT. T. 12 § 1448; Cardtoons, L.C. v. Major League Baseball Players Ass'n, 95 F.3d 959 (10th Cir. 1996)); Pennsylvania (PA ANN. STAT. T. 42 § 8316; Hogan v. A.S. Barnes & Co., Inc., 1957 WL 7316 (Pa. Ct. Pleas 1957; Lewis v. Marriott Intern., Inc., 527 F. Supp. 2d 422 (E.D. Pa. 2007)); Tennessee (TN CODE ANN. § 47-25-1101 et seq. ; State ex rel. Elvis Presley Intern. Mem'l Found. v. Crowell, 733 S.W.2d 89 (Tenn. Ct. App. 1987)); Texas (TX CODE § 26.001 *et seq.*; Kimbrough v. Coca-Cola/USA, 521 S.W.2d 719 (Ct. Civ. App. Tex. 1975)); Utah (UT CODE § 45-3-1 *et seq.*; Nature's Way Prods. v. Nature-Pharma, Inc., 736 F. Supp.245 (D. Utah 1990); Washington (WA STAT. § 63.60.010; State ex rel LaFollette v. Hinkle, 229 P.317 (Wash. 1924)); Wisconsin (WI STAT. § 995.50; Hirsch v. S.C. Johnson & Son, Inc., 90 Wis.2d 379 (1979)).

[125] *See* Jennifer Rothman, Rothman's Roadmap to the Right of Publicity, https://rightofpublicityroadmap.com/law/ (last visited Oct. 15, 2024).

name or image.[126] Other states protect additional aspects of identity, such as gestures and mannerisms, as in Indiana,[127] or "any attribute of an individual that serves to identify that individual to an ordinary, reasonable viewer or listener," as in Illinois.[128] In other states, the law is drafted narrowly, limiting protections to specific groups such as professional performers or soldiers,[129] or to commercial uses. [130]

While most state statutes do not specify rules for secondary liability, courts have generally 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.[131] Several states explicitly limit liability for certain types of intermediaries where they lack knowledge of the unauthorized use. For example, California, Pennsylvania, Ohio, and New York exempt advertising media from liability so long as they do not have knowledge that the use of the name, image, or likeness is unauthorized.[132] Moreover, several courts have found intermediaries not liable for state right of publicity violations where they served as "mere conduits" for the unlawful activity.[133]

In the context of AI, the right of publicity could be a critical legal tool for addressing unauthorized digital replicas. Indeed, to the extent AI-generated deepfakes did not already fit within the existing right of publicity laws, states are amending their laws or enacting new ones specifically to address

[126] White v. Samsung Electronics America, Inc., 971 F.2d 1395, 1399 (9th Cir. 1992).
[127] IND. CODE § 32-36-1-6.
[128] 765 ILL. COMP. STAT. 1075/5.
[129] *See, e.g.,* AZ STAT. §§ 12-761, 13-3726.
[130] The Oregon Supreme Court holds that if a person with an economically valuable identity has her name or image used for commercial purposes there is a cause of action. *See* Anderson v. Fisher Broad. Co., 712 P.2d 803 (Or. 1986).
[131] *See, e.g.*, Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1183–84 (C.D. Cal. 2002); Keller v. Elecs. Arts, Inc., No. 09-cv-1967, 2010 WL 530108, at *3 (N.D. Cal. Feb. 8, 2010) (allowing civil conspiracy claims for violation of California right of publicity to proceed based on defendant's alleged direction of users to infringing websites).
[132] *See* CAL. CIV. CODE §§ 3344(f), 3344.1(a)(l) (West 2024); 42 PA. STAT. AND CONS. STAT. § 8316(d) (2024) (described as those "in the business of producing, manufacturing, publishing or disseminating material for commercial or advertising purposes by any communications medium"); OHIO REV. CODE ANN. § 2741.02(E) (West 2024); N.Y. CIV. RIGHTS LAW § 50-f(9) (McKinney 2024) (adding a "by prior notification" element to knowledge).
[133] *See, e.g.*, Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 27–28 (1st Cir. 2016) (upholding dismissal of statutory misappropriation claims against a classifieds website for images appearing in an advertisement, as it is a "mere[] conduit" and does not benefit from the appropriation); Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1326 (11th Cir. 2006) (highlighting that Amazon did not make "editorial choices" when displaying a book cover that included an unauthorized image on the book's sales page, and that the display was incidental to its role as an internet bookseller).

AI-generated content. California, New York, and Tennessee are among the most recent to pass Right of Publicity legislation.

New York and California recently expanded their right of publicity laws to include AI-generated digital replicas, but the expanded protections are limited to professional performers.[134] In March 2024, Tennessee passed the *Ensuring Likeness, Voice, and Image Security Act of 2024 (ELVIS Act)*, making it one of the first states to directly regulate the misappropriation of identity through generative AI.[135] This law expands liability beyond those who create AI deepfakes to include creators, distributors, and developers of tools such as software and algorithms used to create AI-generated content.[136] This includes AI services and online platforms. The law also expands existing remedies, allowing for injunctive relief, actual damages (including profits), and attorney's fees.[137]

Several states, including Illinois, Kentucky, and Louisiana, have also proposed laws targeting AI-generated digital replicas. Illinois' proposal seeks to amend the state's Right of Publicity Act to provide a civil remedy for simulations of individuals' attributes created through AI.[138] The proposed legislation in Kentucky seeks to regulate the commercial use of an individual's identity through AI-generated content, [139] while Louisiana's would expand protections for political candidates.[140]

Courts have already begun to hear First Amendment challenges involving right of publicity claims in the context of AI. For example, in *Andersen v. Stability AI Ltd*., the Northern District of California, though it dismissed the claim, allowed a plaintiff, a visual artist, to amend her complaint to allege that her "artist identity" had been misappropriated by use in AI training models.[141] Similarly, in *In re Clearview AI, Inc. Consumer Privacy Litigation*, the Eastern District of Illinois found that a class of plaintiffs adequately stated right of publicity claims based on Clearview AI's

[134] SB S7676, Digital Replicas Contract Act, NY Leg. Sess. (2023-2024); AB 2602, CA Leg. Sess. (2023-2024); AB 1863, CA Leg. Sess. (2023-2024).
[135] HB 2091, Ensuring Likeness, Voice, and Image Security Act of 2024, 113th Gen. Assembly (2024).
[136] Prior to the amendment, Tennessee's existing right of publicity law, the Personal Rights Protection Act of 1984, Tenn. Code § 47-25-1101 *et seq*. (TPRPA), prohibited the "unauthorized use" of an individual's "name, photograph, or likeness" for a "commercial purpose."
[137] Supra n.129.
[138] HB 4875, 103rd Gen. Assembly (2023-2024).
[139] SB 317, An act relating to commercial rights to the use of names, voices, and likenesses, 2024 Leg. Sess.
[140] SB 217, 2024 Leg. Sess.
[141] 23-cv-00201-WHO (N.D. Cal. Oct. 30, 2023).

alleged use and scraping of their online photographs, which the court deemed to be sufficiently commercial activity.[142]

These cases highlight the growing reliance on right of publicity laws to address AI-driven misappropriation of identity. As more states introduce legislation, we can expect a rise in right of publicity claims involving AI-generated content.

3. Nonconsensual Distribution of Sexual Images

The problem of AI-generated deepfakes became a topic of national conversation in January 2024 after sexually explicit AI-generated images of Taylor Swift were posted to X.[143] Despite the eventual removal of the images, they were quickly reposted across various accounts and platforms, causing significant harm.[144] This incident, and others like it, underscore the challenges in combating deepfakes and in containing the resulting damage. With this understanding, states have proposed and enacted legislation to regulate nonconsensual distribution of deepfake images and videos.

Laws specifically banning nonconsensual sexually explicit AI-generated images and videos of real individuals date back to 2019, when Virginia became the first state to amend its "revenge porn" law to include sexual deepfakes.[145] Violations of this statute can result in up to a year in jail, a $2,500 fine, or both. California followed suit in 2019,[146] and lawmakers in Hawaii[147] and Georgia[148] introduced similar laws in 2021.

---

[142] In Re: Clearview AI, Inc., Consumer Privacy Litigation, No. 1:2021cv00135 - 314 (N.D. Ill. 2022).
[143] The images amassed over 45 million views, 24,000 reposts, and hundreds of thousands of likes and bookmarks in the 17 hours they were available online. Kate Conger & John Yoon, Explicit Deepfake Images of Taylor Swift Elude Safeguards and Swamp Social Media, NEW YORK TIMES (Jan. 26, 2024), available at https://www.nytimes.com/2024/01/26/arts/music/taylor-swift-ai-fake-images.html
[144] Id.
[145] The update added "falsely created videographic or still image" to the existing language. VA. CODE ANN. § 18.2-386.2 (2019).
[146] The law allows victims of deepfake pornography to sue those who create and distribute sexually explicit deepfake material if the victim did not consent to it. Victims can sue for up to $150,000 if the deepfake was "committed with malice." AB 730, 2019 – 2020 Leg., Reg. Sess.
[147] The bill outlawed the intentional creation, disclosure, or threat of disclosure of nonconsensual sexually explicit deepfake images or videos, making it a Class C felony punishable by up to five years imprisonment and a fine of up to $10,000. SB 309, 2020 – 2021 Leg., Reg. Sess.
[148] The law banned the online dissemination of falsely created pornographic images or videos. SB 78, 2021-2022 Leg. Reg. Sess.

In 2022, South Dakota made it a misdemeanor to create nonconsensual deepfake pornography, elevating the offense to a felony if the victim is under 17 and the perpetrator is at least 21.[149] Offenders face up to two years in prison, a $4,000 fine, or both.[150] Similarly, Florida passed a law prohibiting the dissemination of nonconsensual sexual deepfakes, with violations punishable as a third-degree felony carrying a maximum sentence of five years in prison, a $5,000 fine, and 5 years of probation. [151]

The momentum continued in 2023, with 5 states–Illinois, California, Texas, New York, and Minnesota–passing laws to address deepfakes.[152]

In 2023, state laws also began to distinguish between sexual deepfakes targeting adults and AI-generated content depicting children, with states like Louisiana and Texas adding AI-generated content to their existing CSAM laws.[153] 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.[154]

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 nonconsensual sexually explicit deepfakes, either in conjunction with or independent of specific anti-deepfake criminal

[149] SD CODE § 22-21-4.
[150] Id.
[151] SB 1798, 2022 Leg., Reg. Sess.
[152] SB 382, 2023-204 103rd Leg. Sess. (adding the term "digitally altered sexual image" to the Illinois Remedies for Nonconsensual Dissemination of Private Sexual Images Act); CA CODE § 1708.85; SB 1361, 2023 Leg., Reg. Sess. (adding the term "deepfake video"); SB S1042A, 2023-2024, Leg., Reg. Sess. (codified at NY PENAL CODE §245.15); HB 1370, 93rd Leg. Sess. (2023-2024) (making it illegal to create sexually explicit deepfakes with violators subject to five years in prison and $10,000 in fines for distributing the images or videos (MN STAT. 617.261)).
[153] SB 175, Leg. Sess. (2023); HB 2700, 88th Leg. Sess. (2023).
[154] HB 575, 67th Leg. Sess. (2024); HB 1126, Walker Montgomery Protecting Children Online Act, 2024 Leg. Sess.; SB 79, 99th Leg. Sess. (2024) (adding computer-generated content to "child pornography" law); HB 2163, 2024 Leg. Sess. (specifying that for the purposes of sexual exploitation of children offenses, the term "material" includes computer-generated images created, adapted, or modified by artificial intelligence); HB 1999, 68th Leg. Sess. (2023-2024) (adding "fabricated depiction of a minor" and defining "digitization" to include creation or alteration of any visual or printed matter by using artificial intelligence software); SB 1680, 2024 Leg. Sess. (adding "generated child pornography" to the definitional provision); HB 207, 2024 Leg. Sess. (adding "computer-generated images" including those created, adapted, or modified by a computer to appear to be an identifiable person and explicitly providing that the minor need not actually exist); HB 3642, 2024 Leg. Sess. (expanding the definition "visual depiction" to include computer-generated images that have been adapted, altered, or modified to make it appear as though a minor is engaging in sexually explicit conduct); SB 2243, 2023-2024 Leg. Sess. (adding digitally altered images and videos to the definition of "child pornography."); HB 993, 2024 Leg. Sess. (specifying that the existing statute covers visual materials that have been created, adapted, or modified to make it appear as though an identifiable minor is engaging in sexually explicit conduct); SB 713, 2024 Leg. Sess.

statutes.[155] In states without such 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.[156] Thirty of those states have criminal laws that explicitly prohibit the distribution of nonconsensual sexual deepfakes.[157] Twenty-two of those states prohibit the distribution of nonconsensual deepfakes if the defendant acted with a specific intent (e.g., to harass or intimidate)

---

[155] CA CODE § 1708.85 (providing for a civil cause of action for any person who suffers harm to recover an amount equal to the monetary gain made by the defendant from the creation, development, or disclosure of the material and either economic and noneconomic damages proximately caused by the disclosure of the material, or statutory damages in an amount no less than $1,500 but no more than $30,000 or $150,000 if committed with malice); FL STAT. § 836.13 (providing for a civil cause of action for any aggrieved person to obtain appropriate relief including injunctive relief, the greater of $10,000 or the actual damages incurred, and reasonable attorney's fees and costs); 740 ILCS 190/5 (establishing that a plaintiff may recover the greater of economic and noneconomic damages proximately caused by the defendant's dissemination or threatened dissemination, or statutory damages, not to exceed $10,000, against each defendant for all disseminations and threatened disseminations as well as an amount equal to any monetary gain made by the defendant from dissemination of the private sexual image, punitive damages, reasonable attorney's fees and costs, and injunctive relief); H 1047, 123rd Gen. Assembly (2024) (providing that certain images created by AI or similar means constitute an "intimate image" for purposes of a civil action involving nonconsensual pornography); MN STAT. § 604.32(3)-(4) (permitting a successful plaintiff to recover general and special damages, including all finance losses due to the dissemination of the deep fake and damages for mental anguish, an amount equal to any profit made from the dissemination of the deep fake by the person who intentionally disclosed the deep fake, a civil penalty awarded to the plaintiff of an amount up to $100,000, court costs, fees, and reasonable attorney's fees and injunctive relief).

[156] *See* AL ST §13A-6-240; AK STAT. §11.61.127 (possession of child pornography); AZ STAT § 13-1425; AR CODE § 5-26-314; CA PENAL CODE § 647(j)(4); CO REV. STAT. § 18-7-107 (requires intent to harass, intimidate, or coerce or where such posting results in serious emotional distress); CON. GEN. STAT. § 53a-189c; FL STAT. § 784.049 (cyber sexual harassment); DE CODE T. 11, § 1335 (violation of privacy); GA CODE § 16-11-90 (invasion of privacy); HI ST 711.1110.9 (invasion of privacy); ID CODE 18-6609; IL § 5/11-23.5; IN CODE §35-45-4-8; IA CODE §708.7(1)(a)(5); KS STAT § 21-6101 (breach of privacy); KY STAT. 531.120; LA REV. STAT. §14:283.2; ME STAT §511-A; MD CODE § 3-809; H 4744, An Act to Prevent Abuse and Exploitation, 193rd Leg. Sess. (Massachusetts 2024); MI PENAL CODE § 750.145e; MN STAT 617.261; MS CODE §97-29-64.1; MO STAT 573.110; MT STAT 45-8-213 (privacy in communications); NE STAT 28-311.08 (unlawful intrusion); NV REV. STAT 200.780; NH REV. STAT. § 644:9(III) (violation of privacy); NJ STAT § 2C:14-9 (invasion of privacy); NM STAT § 30-37A-1; NY PENAL CODE §245.15l; NC STAT § 14-190.5A; ND STAT § 12.1-17-07.2; OH REV. CODE § 2917.211; 21 OK STAT §1040.13b; OR REV. STAT.§ 163.472; PA STAT § 3131; RI STAT § 11-64-3; SD STAT 22-21-4 (privacy); TN CODE §39-17-318 (unlawful exposure); TX PENAL CODE §21.16; UT STAT 76-5b-203; VT STAT § 2606; VA STAT § 18.2-386.2; WA REV. CODE § 9A.86.010; WV CODE §61-8-28a; WI STAT § 942.09; WY § 6-4-305; D.C. CODE §22-3052; GUAM P.L. No. 33-171; PR LAWS ACT 21 (P. de la C. 547).

[157] These states include Alabama, Arizona, California, Colorado, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maryland, Massachusetts, Minnesota, Mississippi, New Hampshire, New York, North Carolina, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, and Wisconsin. *See* ALA. CODE §13A-6-240 (2019); A.R.S. § 16-1023; CAL. CODE §647(J)(4); HB 1147, 2024, Leg., Reg. Sess.; HB 353, 2024 Leg., Reg., Sess.; FL STAT. § 784.049; GA CODE § 16-11-90; HI REV. STAT. § 711-1110.9 (2023); ID CODE §18-1514; 720 ILCS 5/11-23.5; IN Code § 35-45-4-8 (2023); IOWA CODE §728.12 (2021); KY REV STAT. § 531.120 (2021); LA REV. STAT. §14:283.2; MD CODE § 3-809; H 4744, 193rd Leg. Sess. (2024); MN STAT. § 617.261; SB 2577, 2024 Leg., Reg. Sess.; NH REV. STAT. § 644:9(III); NY PENAL CODE §245.15; NC STAT. § 14-190.5A; OK STAT. § 1040.13b (2022); SC CODE § 7-25-230; SD CODE § 22-21-4; TN SB 2096 (2024); TX CODE §21.16; UT CODE 76-5b-203; HB 1525, 2024 Leg., Reg., Sess.; WA REV. CODE § 9A.86.010; WI STAT 942.09.

or with some level of knowledge—either actual or imputed through recklessness or negligence—that the depicted person had not consented to the disclosure,[158] while 19 states specifically prohibit the creation of AI-generated CSAM[159], and 11 states cover both the creation and distribution of nonconsensual sexual deepfakes, including AI-generated CSAM.[160] 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.[161] Except for Illinois, courts in these states recognized that the laws regulated speech based on its content and thus were subject to the highest level of judicial scrutiny.[162] The statutes survived strict scrutiny, as the courts concluded they served compelling governmental interests in safeguarding privacy and preventing the psychological and reputational harm caused by the public disclosure of intimate images.[163]

These decisions did not address the potential interaction between these state laws and §230 of the Communications Decency Act. Although §230 does not bar federal criminal law enforcement, it generally 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 a result, it is also likely that such claims would be dismissed early in the litigation process, thus preventing review on the merits.

---

[158] These states include Alabama, California, Delaware, Florida, Georgia, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maryland, Mississippi, New Hampshire, North Carolina, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, Washington, and Wisconsin. *See* infra n. 157.

[159] 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. *See* infra n. 157.

[160] Those states are Alabama, Arizona, Colorado, Delaware, Hawaii, Idaho, Indiana, Massachusetts, Minnesota, New York, and Vermont. *See* infra n. 156.

[161] [9]*See, e.g.*, People v. Iniguez, 202 Cal. Rptr. 3d 237 (Cal. App. Dep't Super. Ct. 2016); People v. Austin, 155 N.E.3d 439, 448–49(Ill. 2019); State of Indiana v. Conner Katz, No. 20S-CR-632, __ N.E.3d__(Ind., Jan. 18, 2022); State v. Casillas, 952 N.W.2d 629, 634 (Minn. 2020); State v. Lamoureux, 485 P.3d 192 (Mont. 2021); Ex parte Jordan Bartlett Jones, 2021 WL 2126172, at *1(Texas); State of Vermont v. Rebekah S. VanBuren, 210 Vt. 293 (2018); State v. Culver, 918 N.W.2d 103 (Wis. Ct. App. 2018).

[162] The Court explained that the Indiana State Constitution ultimately provides less protection to defendants by way of a lower standard of scrutiny than the Federal Constitution. The freedom of expression which is protected under the Indiana State Constitution is qualified by the responsibility clause found in Article 1, Section 9, which provides that "for the abuse of that right, every person shall be responsible." Katz, No. 20S-CR-632 at 8.

[163] *See* infra n. 157.

As of October 2024, at least 37 states are considering legislation to expand their laws targeting the creation and distribution of nonconsensual sexual deepfakes.[164]

C. 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. While these efforts aim to ensure responsible AI deployment, they carry significant implications for combating AI-generated CSAM. Strengthening regulatory frameworks is essential to empower law enforcement, hold offenders accountable, and prevent the exploitation of minors. However, state-level efforts to regulate AI, though well-intentioned, fall short given the nature of AI products and services, which frequently cross both state and national borders. The resulting patchwork of laws creates regulatory confusion, raises compliance costs, and may hinder best practices that protect consumers. A unified federal approach is critical to establishing clear, consistent guidelines and robust protections, ensuring an effective response to AI-related challenges and safeguarding individuals from harm.

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.[165] The framework aims to help individuals, organizations, 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.[166]

---

[164] *See* National Conference of State Legislatures, Deceptive Audio or Visual Media ('Deepfakes') 2024 Legislation, https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation (last visited October 10, 2024).

[165] HR 6216, National Artificial Intelligence Initiative Act of 2020, 116th Congress (2019-2020) (P.L. 116-283).

[166] NAT'L INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T OF COMMERCE, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (July 2024), available at https://www.nist.gov/itl/ai-risk-management-framework.

The White House Office of Science and Technology Policy took this guidance a step further with its *Blueprint for an AI Bill of Rights*.[167] 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.[168] Notably, it emphasizes 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.[169] In 2023, the Biden-Harris Administration secured commitments from leading AI developers to publicly evaluate their AI systems.[170]

President Biden recently issued an *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.*[171] This order coordinates efforts across the federal government to promote responsible innovation, protect privacy and civil liberties, safeguard American workers, and manage the risks posed by AI.[172] Together, these initiatives lay a strong foundation for advancing ethical AI practices and ensuring that AI technologies are developed and deployed responsibly across the nation.

ii. The State Regulatory Frameworks

Jurisdictions across the United States are increasingly enacting or exploring legislation to address the growing risks posed by AI technologies, including concerns related to deepfakes, algorithmic bias, and potential harm to users across industries. 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

---

[167] WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (October 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[168] Id.
[169] Id.
[170] Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI, WHITEHOUSE.GOV (July 21, 2023), 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/
[171] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, WHITEHOUSE.GOV (Oct. 30, 2023), 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/
[172] Id.

bills.[173] 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.[174]

At least 12 states— California,[175] Connecticut,[176] Florida,[177] Illinois,[178] Louisiana,[179] New York,[180] Oregon,[181] Pennsylvania,[182] Rhode Island,[183] Texas, [184] Utah,[185] Vermont,[186] and Washington[187]— have prioritized protecting 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, which is responsible for, among other things, identifying any potential adverse impacts of the state's AI systems on residents.[188] As part of this effort, the division is required to propose a state code of ethics on the use of AI.[189] Washington's task force is charged with identifying the benefits and risks of AI systems broadly but is required to give close consideration to the impact on historically marginalized

[173] National Conference of State Legislatures, Artificial Intelligence 2024 Legislation, https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation (last updated Sep. 9, 2024).
[174] Id.
[175] AB 302, An act to add Section 11546.45.5 to the Government Code, relating to automated decision systems, 2023 Leg. Sess.
[176] Public Act No. 23-16.
[177] SB 1680, 2024 Leg. Sess.
[178] HB 3563, 103rd Gen. Assembly (2023) (Public Act 103-0451)
[179] HCR 66, An act to provide for a joint legislative committee to study regulations regarding AI, 2024 Leg. Sess.
[180] SB 3971, 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 Leg. Sess. (2019-2020).
[181] H4153, 82nd Leg. Sess. (2024).
[182] HR 170, 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 Leg. Sess.
[183] SJR 14, 2024 Leg.
[184] HB 2060, 88th Leg. Sess. (2023).
[185] SB149, 2024 Leg. Sess.
[186] HB 378, An act relating to the creation of the Artificial Intelligence Task Force, 2018 Leg. Sess.
[187] SB 5838, Artificial Intelligence Taskforce, 68th Leg. Sess. (2024).
[188] Supra n. 186.
[189] Id.

communities.[190] 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. [191] 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. [192]

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.[193]

These states focus on giving consumers the ability to opt-out of profiling in cases where automated decisions could significantly affect them, such as in areas like health care, education, or financial services. Colorado's legislation stands out by requiring developers of high-risk AI systems to prevent algorithmic discrimination and disclose AI use to consumers.[194]

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.[195] 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.[196]

---

[190] Supra n. 187.
[191] SB8209, 2024 Leg. Sess.
[192] HB72, MA 193rd Gen. Assembly (2023-2024); SB 2545, NJ 2024 Leg. Sess.
[193] 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.).
[194] SB21-190, 73rd Gen. Assembly (2021).
[195] *See* infra n. 225.; *see also* SB 5092, WA Leg. Sess. (2021-2022).
[196] HB 1181, 2023 Leg. Sess. (Pub. Ch. 408

Legislation has also been introduced in at least a dozen additional states. For example, 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.[197] 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.[198]

In response to growing concerns over AI-generated explicit content, states such as California,[199] Utah,[200] Arkansas,[201] Virginia,[202] Mississippi,[203] and Louisiana[204] have enacted stricter age-verification requirements for platforms hosting explicit material. Notably, Utah and Arkansas expanded their definitions of 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.[205]

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 noncompliance.[206]

As new state AI regulations emerge, a key challenge has been defining what constitutes a "developer" of an AI system. Unlike static software, AI evolves through additional training over time, raising questions about when modifying or fine-tuning a model turns a user into a developer subject to regulation. Colorado's law, the first AI model development-focused law to pass, offers one approach. 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."[207] Meanwhile, California's law uses

[197] H747, 2024 Leg. Sess.
[198] H7786, 2024 Leg. Sess.; H 7521/ S 2888, 2024 Leg. Sess.
[199] AB 2273, The California Age-Appropriate Design Code Act, Leg. Sess. (2023-2024).
[200] SB 287, 2023 Leg. Sess.
[201] Act 689 of 2023.
[202] SB 1515, Reg. Leg. Sess. (2023-2024).
[203] SB 2346, 2023 Leg. Sess.
[204] HB 142, Act No. 440, 2022 Leg. Sess.
[205] 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).
[206] SB 1047, Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, Reg. Leg. Sess. (2023-2024).
[207] SB 205, 2024 Leg. Sess. (May 17, 2024).

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.[208] 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.

IV. ANALYSIS: AI-GENERATED CSAM: LEGAL AND REGULATORY FRAMEWORKS IN CANADA

The Canadian Criminal Code provides robust federal protections against all forms of child exploitation, including AI-generated CSAM. As in the United States, Canada classifies both CSAM and obscenity as prohibited, non-protected speech, making laws that criminalize the production, distribution, and possession of such content the primary legal mechanisms for combating AI-generated CSAM. The Criminal Code also includes protections against the non-consensual distribution of intimate images, which may be invoked to combat morphed images and other malicious uses of AI technologies. Federal privacy and copyright laws may also provide limited protections to victims. While the federal government has exclusive jurisdiction in criminal law, the provinces control much of civil law and have enacted laws to provide victims with meaningful redress for privacy and other related violations.

A. THE FEDERAL LEGAL FRAMEWORK

i. Canadian Criminal Code Offenses

1. Child Pornography

In Canada, the regulation of CSAM is primarily governed at the federal level under the Canadian Criminal Code, which applies uniformly across all provinces and territories. Although the Code does not explicitly address AI-generated content, Section 163.1 of the Code covers access, possession, creation, and distribution of "child pornography," which is defined broadly to include any visual representation, including those made by "electronic or mechanical means," that depicts a "person" who is or is represented as a minor engaging in "sexual activity," or the "dominant characteristic" of which is, "for a sexual purpose," the exhibition of a minor's genitals or anus.[209]

[208] Supra n. 207.
[209] R.S.C., 1985, c. C-46 s. 163.1(a)(1).

This definition extends beyond visual depictions to include written material, audio recordings, and other representations that advocate or counsel sexual activity with a minor that would be an offense under the Criminal Code.[210]

The penalties for "child pornography" offenses in Canada are severe, reflecting the gravity of the harm caused by CSAM. If prosecuted as an indictable offense, the creation, distribution, or sale of CSAM carries a maximum sentence of 14 years in prison, with a mandatory minimum of 1 year. [211] Possession and viewing offenses, when treated as indictable offenses, are punishable by up to 10 years in prison with a minimum of 1 year. [212] Aggravating factors, such as intent to profit or involvement of particularly young victims, may result in harsher sentences, with offenders also subject to mandatory registration on the National Sex Offender Registry. [213]

Persons and organizations that provide internet services must also report tips regarding websites that may contain CSAM to the Canadian Centre for Child Protection and law enforcement if they believe a CSAM offense has been committed using their service.[214] Failure to report can result in fines of up to $10,000, or $100,000 for repeat violations, and 6 months imprisonment for individuals.[215]

Application of the "child pornography" statute to AI-generated CSAM relies, in significant part, on the definition of "person" as used in section 163.1(a)(1) and whether the term is limited to actual persons or if it covers fictitious minors as well. On this, the Supreme Court of Canada has said:

> "The available evidence suggests that explicit sexual materials can be harmful whether or not they depict actual children. Moreover, with the quality of contemporary technology, it can be very difficult to distinguish a "real" person from a computer creation or composite. Interpreting 'person' in accordance with Parliament's purpose of criminalizing possession of material that poses a reasoned risk of harm to children, it seems that it should include visual works of the imagination as well as depictions of actual people. Notwithstanding the fact that 'person' in the charging section and in s. 163.1(1)(b) refers to a flesh-and-

[210] R.S.C., 1985, c. C-46 s. 163.1(b)-(d).
[211] R.S.C., 1985, c. C-46 s. 163.1(2)-(3).
[212] Id at s. 163.1(4),(4.1).
[213] R.S.C., 1985, c. C-46 s. 163.1(4.3).
[214] S.C. 2011, c. 4.
[215] S.C. 2011, c. 4.

> blood person, I conclude that 'person' in s. 163.1(1)(a) includes both actual and imaginary human beings."[216]

In *R v. Sharpe*, the Canadian Supreme Court upheld the constitutionality of the Code's "child pornography" provision, finding that its application to depictions of fictitious minors was justified under the *Canadian Charter of Freedoms.*[217] However, the Court carved out two exceptions to the possession provision where regulation could not be justified under the *Charter*: 1) self-created, privately held works of imagination and 2) lawfully created visual recordings of consensual sexual activity involving the possessor and held for private use.[218] These exceptions do not insulate individuals who possess such materials with the intent to distribute them, which the Court has recognized inflicts unique injuries on victims whose images can circulate indefinitely online."[219]

In its decision, the Court emphasized that regulation is constitutionally justifiable if the impact of the type of material in question poses a "reasonable risk" of harm to children.[220] The Court articulated four categories of harm that section 163.1 was intended to prevent: 1) child sexual abuse and exploitation of children who are used in the production of CSAM and whose images are disseminated over time; 2) normalizing deviant sexual behavior that increases the risk of physical harm to children; 3) fueling fantasies that incite violence against children; and 4) the use of CSAM to groom children in order to facilitate physical sexual offenses against them.[221] This harm analysis, which focuses on the increased risk of *physical* harm to children, has created some ambiguity regarding the extent to which the freedom of expression under the Charter can be limited in the context of AI-generated CSAM.

In 2023, a Provincial court in Quebec sentenced a man to over 3 years in prison for using deepfake technology to produce synthetic videos of children being sexually assaulted, making it the first case in the country to address AI-generated CSAM.[222] The judge ruled that the material's

---

[216] R. *v.* Sharpe, [2001] 1 S.C.R. 45, ¶38 2001 SCC 2.
[217] Id.
[218] Id at ¶76; *see also* R v Barabash, [2015] SCC 29 (holding that any exemptions to the law were only valid if no factual exploitation or abuse of children was involved in creating the materials.).
[219] Id.
[220] Id.
[221] Id at ¶85-94.
[222] Jacob Serebrin, Quebec man who created synthetic, AI-generated child pornography sentenced to prison, THE CANADIAN PRESS (Apr. 26, 2023), https://www.cbc.ca/news/canada/montreal/ai-child-abuse-images-1.6823808.

indistinguishability from real CSAM created comparable risks by "fueling fantasies that incite sexual offenses against children."[223]

Although litigation involving AI-generated CSAM remains limited in Canada, evolving jurisprudence suggests a willingness to interpret "child pornography" laws broadly to address synthetic content, recognizing that the harm caused by AI-generated CSAM lies not only in the content itself but also in how it perpetuates exploitation.

2. Obscenity

Section 163 of the Criminal Code governs offenses related to the creation and distribution of "obscene" material." [224] The statute does not proscribe pure possession. The core of these prohibitions is found in Section 163(8), which defines "obscene material" as any matter of which the "dominant characteristic" is the "undue exploitation of sex," or a combination of sex and either crime, horror, cruelty, or violence.[225] Notably, Section 163(5) removes intent from consideration—if the material meets the definitional threshold, it constitutes an offense punishable by up to two years imprisonment.[226]

The potential applicability of these provisions to AI-generated CSAM is guided by the principles set forth by the Supreme Court in *R v. Butler*. In this landmark decision, the Court evaluated whether the legal definition of obscenity infringes on the right of free expression under Section 2(b) of the *Canadian Charter of Rights and Freedoms*. [227] In order to qualify as obscene, the exploitation of sex must not only be its dominant focus, but such exploitation must also be "undue." To aid in the Court's analysis, Justice Sopinka articulated three categories of potentially obscene materials:

1. Explicit sex with violence, which almost always meets the threshold of obscenity.
2. Explicit sex without violence but involving degradation or dehumanization, which qualifies if it poses a substantial risk of harm.

[223] Id.
[224] RSC 1985, c C-46, s 163.
[225] Id at s 163(8).
[226] RSC 1985, c C-46, s 169. An obscenity charge is a hybrid offense that can be treated as either a summary offense (minor crimes) or an indictable offense (major crimes), depending on prosecutorial discretion.
[227] R. v. Butler, 1992 CanLII 124 (SCC), [1992] 1 SCR 452.

3. Explicit sex without violence, degradation, or dehumanization, which is generally tolerated unless it involves minors.[228]

The Court applied the community standards of tolerance test, evaluating what society deems others should not be exposed to, along with the internal necessities test, which exempts material with legitimate artistic, scientific, or literary value.[229] The Court ultimately upheld Section 163, clarifying that the purpose of the law was not "moral condemnation" but rather "the prevention of harm to society," particularly the influence that degrading sexual material can have on public attitudes toward women and children. [230] In his concurring opinion, Justice Gonthier added that even seemingly innocuous content could create a substantial risk of harm if its representation normalizes sexual activity with minors.[231]

Similarly, AI-generated CSAM can blur boundaries around the acceptability of sexualizing minors, reinforcing dangerous ideologies that could lead to real-world abuse. As with traditional obscenity laws, the focus of regulation must remain on the harmful influence of such material on societal norms, rather than the presence of real individuals.

The broad language of Section 163 suggests that AI-generated CSAM could fall within its ambit, although Canadian courts have yet to address this issue directly. The reliance on subjective community standards to determine what constitutes obscenity introduces a degree of unpredictability, with enforcement varying between provinces. This inconsistency highlights the need for clearer legal criteria to address evolving forms of digital exploitation, particularly as AI technologies continue to advance.

3. Non-consensual Publication of Intimate Images

[228] Id at 475.
[229] Id.
[230] Id.
[231] Id at 485, 519. (Gonthier J., Concurring) ("I would hold that materials falling within Sopinka J.'s third category (explicit sex with neither violence nor degradation or dehumanization), while generally less likely to cause harm than those of the first two categories, may nevertheless come within the definition of obscene at s. 163(8) of the *Code*, if their content (child pornography) or their representational element (the manner of representation) is found conducive of harm.").

To address emerging online threats and better protect victims, Canadian lawmakers, in 2015, passed the *Protecting Canadians from Online Crime Act* .[232] This legislation amended the Criminal Code by adding Section 162.1, which prohibits the non-consensual publication, distribution, and sale of intimate images, and Section 164.1, which empowers courts to order the removal and destruction of such content, including CSAM, voyeuristic recordings, and advertisements for sexual services, whether distributed through print media or via digital platforms.[233] To secure a conviction, the prosecution must prove that the defendant knowingly or recklessly distributed the image without the consent of the individual depicted.[234]

Section 162.1(2) defines an "intimate image" as a visual image or recording, created by any means, of a person who is nude, exposing their genitals or breasts, or engaged in sexual activity.[235] In *R v. Verner*, the Ontario Court of Justice clarified that the elements under the definition of an "intimate image" are to be understood disjunctively. That is, an image may be proscribed if it depicts *either* nudity, exposure of the genitals or breasts, *or* sexual activity.[236] This definition also requires that, at the time the image was taken, the circumstances gave rise to a reasonable expectation of privacy, and that the person depicted maintains this expectation when the offense occurs.[237]

While these provisions explicitly reference photographic, film, or video recordings, their application to deepfake pornography remains open to judicial interpretation. In the context of AI-generated CSAM, the key legal questions would be whether the content meets the statutory definition of an "intimate image" (likely) and whether the child depicted has a reasonable expectation of privacy with regard to the photo (less likely).

As courts begin to interpret these statutes in the context of evolving AI technologies, the ability to criminalize and remove AI-generated CSAM will depend on how concepts like consent, reasonable expectation of privacy, and distribution are applied to synthetic content.

[232] Bill C-13, Protecting Canadians from Online Crime Act, 2nd Sess., 41st Parl. (2015).
[233] Criminal Code, RSC, 1985, c. C-46, s 162.1, 164.1.
[234] Id at s 162.1.
[235] Id at s 162.1(2).
[236] R v Verner, 2017 ONCJ 415 at ¶6.
[237] Id at s 162.1(2)(b)-(c).

ii. Privacy Legislation

Privacy legislation is critical in addressing the risks posed by AI systems, particularly those employing deepfake technologies. When AI-generated outputs expose personal or sensitive information without consent, it may constitute a privacy violation and, in some cases, be subject to sanctions under federal and provincial laws.

At the federal level, the *Personal Information Protection and Electronic Documents Act (PIPEDA)* establishes guidelines for how private-sector entities must collect, use, and disclose personal information while engaged in commercial activities. [238] Provinces such as Alberta, British Columbia, and Quebec have enacted their own private laws that apply to the private sector that are considered substantially similar to the PIPEDA. As a result, organizations operating under these provincial jurisdictions are typically exempt from PIPEDA's requirements concerning intra-provincial activities. [239]

Under the PIPEDA, the collection, use, or disclosure of personal information must be consistent with what a "reasonable person" would consider appropriate under the circumstances. [240] The Office of the Privacy Commissioner of Canada (OPC) emphasizes that managing personal information in illegal or potentially harmful ways is inherently inappropriate. [241] Personal information is broadly defined to include both factual and subjective data about an identifiable individual. [242] Sensitive information—such as biometric data,[243] details related to an individual's

[238] Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5
[239] Personal Information Protection Act, SA 2003, c P-6.5 (Alberta); Personal Information Protection Act, SBC 2003, c 63 (British Columbia); An act respecting the protection of personal information in the private sector, c P-39.1 (Quebec); other provinces such as Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador have adopted similar legislation governing personal health information.
[240] Office of the Privacy Commissioner Canada, PIPEDA fair information principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/ (last visited Oct. 10, 2024).
[241] Id.
[242] Id.
[243] Office of the Privacy Commissioner Canada, PIPEDA Report of Findings #2021-001, Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the *Commission d'accès à l'information du Québec*, the Information and Privacy Commissioner of British Columbia, and the Information of the Privacy Commissioner of Alberta, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

sexual practices or preferences,[244] and information that could affect one's reputation[245]—requires additional protection due to its potential to cause long-term harm if compromised.

Investigations into tech companies relating to safeguarding failures are already well underway. In 2023, an investigation by the OPC into MindGeek, the parent company of Pornhub, revealed that the company violated the PIPEDA by relying on users to verify consent when uploading intimate images without conducting independent checks.[246] The investigation also found that the company lacked effective mechanisms to remove content and prevent re-uploads, thereby exacerbating harm to victims.[247] The OPC's recommendations included a call for the company to cease collecting and disclosing user-generated intimate images until valid consent could be obtained directly from each individual featured in such content and confirm that the individuals were of legal age to provide such consent.[248]

Additionally, in response to emerging risks of AI technologies, both the OPC and provincial privacy regulators, issued the *Principles for Responsible, Trustworthy, and Privacy-Protective Generative AI Technologies (Generative AI Guidance*).[249] This guidance interprets existing privacy laws in relation to generative AI systems and underscores the importance of obtaining explicit consent when utilizing personal information to train or deploy these technologies.[250] The guidance discourages the use of data scraping to collect personal information without consent,

[244] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2016-005, Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/.
[245] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2013-003, Profiles on PositiveSingles.com dating website turn up on other affiliated dating websites, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-003/; PIPEDA Report of Findings #2016-005, Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/.
[246] Office of the Privacy Commissioner of Canada, Pornhub operator failed to obtain meaningful consent before allowing adult content to be posted on its websites (Feb. 29, 2024), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/nr-c_240229/
[247] Id.
[248] Id.
[249] Office of the Privacy Commissioner of Canada, Principles for responsible, trustworthy and privacy-protective generative AI technologies, (Dec. 7, 2023) https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/.
[250] Id.

which is critical given that these datasets frequently include identifiable information.[251] Notably, it anticipates that the creation of nonconsensual deepfakes will be prohibited, though courts have not issued definitive ruling on many AI-related privacy issues.[252]

iii. Copyright Law

Advancements in machine learning and data mining have enabled AI systems to generate content that mimics human-created works, raising important questions about authorship and ownership under Canadian copyright law. Traditionally, Canadian law requires a "natural person exercising skill and judgment" to qualify as the creator of a work. [253] While individuals may meet this threshold in AI-assisted works, those issuing simple prompts to generative AI systems like ChatGPT are less likely to qualify. As Canada explores amendments to the Copyright Act, questions of ownership and control over AI-generated content become critical for assigning liability.

Liability concerns extend to both primary infringement, which requires access, reproduction, and substantial copying of original works, as well as secondary infringement, which occurs when an individual knows or should have known that a work was infringing material and undertakes an additional act in relation to that work in violation of the Copyright Act.[254] In the context of CSAM, users may face secondary liability if they prompt AI systems to create explicit or harmful content and then share it with other users. However, without a clear framework for authorship, it remains difficult to determine whether accountability lies with the user, developer, or the service provider.

The use of data mining techniques to train AI models further complicates the legal landscape. This process involves copying and analyzing extensive datasets which often contain copyrighted material to identify patterns and generate predictions.[255] In Canada, there are two primary exceptions to copyright infringement that might apply to data mining activities: 1) fair dealing, which allows limited use of copyrighted materials for research; and 2)the technological process

[251] Id.
[252] Id.
[253] *See* CCH Canadian Ltd. v. Law Society of Upper Canada, [2004] 1 S.C.R. 339 at para. 16 [CCH].
[254] Government of Canada, Copyright infringement, https://ised-isde.canada.ca/site/canadian-intellectual-property-office/en/copyright-infringement (last updated Mar. 19, 2021).
[255] Michelle Chen, A Guide: Text Analysis, Text Analytics & Text Mining, TOWARDS DATA SCIENCE (Oct. 21, 2020), https://towardsdatascience.com/a-guide-text-analysis-text-analytics-text-mining-f62df7b78747.

exception, which applies to material created automatically during technological operations that are erased after completion.[256] Canadian courts have applied the fair dealing principle in relation to a "web-crawler" that gathered text and photos from websites for inclusion on the defendant's own website.[257] The court ruled that this automated replication constituted copyright infringement, though its unclear if similar reasoning would apply to data mining activities used to train AI models.[258]

Regarding the technological processes exception, the Canadian Copyright Board has interpreted this provision as applicable only to "copies that happen automatically, or without the direct control of the user," that are then automatically deleted upon completion.[259] As is true in the context of fair dealing, there is significant uncertainly regarding whether and to what extent this exception would apply to AI-related data mining activities. For example, while some data mining activities may require temporary copies to be made, others may require that copies of works be stored indefinitely, which would make this provision inapplicable.

These uncertainties in copyright law raise critical issues when applied to the context of AI-generated CSAM. AI systems trained on datasets scraped from the internet—without proper consent or oversight mechanisms in place—could inadvertently produce explicit content featuring the likeness of real children. Liability for such content remains difficult to assign, as it is unclear whether responsibility rests with the developer, user, or the AI system itself. Additionally, proving infringement becomes more complex when AI-generated outputs resemble existing copyrighted works but are created through automated processes. Courts will likely soon be asked to grapple with these questions regarding liability.

The issue of AI authorship is currently before Canada's Federal Court following a controversial decision by the Canadian Intellectual Property Office (CIPO) to grant a copyright registration for an AI-generated image titled *Suryast*, which combined a photograph of a sunset with Van Gogh's

[256] Copyright Act, R.S., 1985, c. C-42, s. 29
[257] *See* Century 21 Canada Limited Partnership v Rogers Communications Inc., 2011 BCSC 1196, online: CanLII https://www.canlii.org/en/bc/bcsc/doc/2011/2011bcsc1196/2011bcsc1196.pdf; *see also* Trader v CarGurus, 2017 ONSC 1841, online: CanLII https://www.canlii.org/en/on/onsc/doc/2017/2017onsc1841/2017onsc1841.html.
[258] Id.
[259] *See* SOCAN, Re: Sound, CSI, Connect/SOPROQ, Artisti – Tariff for Commercial Radio, 2011-2017 (2016), at para. 175-186, online: Copyright Board https://decisions.cb-cda.gc.ca/cb-cda/decisions/en/366778/1/document.do.

painting *The Starry Night.* If upheld, the registration raises the possibility that developers or users could claim ownership of AI outputs, and potentially avoid liability by shifting responsibility for the misuse of their systems to other actors involved in the content's generation and distribution.

Ultimately, the unresolved intersection of authorship and liability demonstrates the need for clearer legal standards. Without a coherent framework linking ownership, authorship, and liability, victims of AI-generated CSAM may struggle to pursue legal remedies, while developers and users could evade accountability for the exploitation facilitated by their systems.

B. PROVINCIAL LEGAL FRAMEWORKS

Provinces play a relatively narrow role in the regulation of "child pornography" and "obscenity" because criminal law falls exclusively within federal jurisdiction. However, provincial agencies are responsible for enforcing the *Criminal Code* provisions within their jurisdictions. While criminal law is federally governed, civil laws at the provincial level—namely privacy and nonconsensual distribution of intimate images laws —provide an important avenue for victims to seek redress.

i. Non-Consensual Distribution of Intimate Images

In Canada, 8 provinces and territories have enacted legislation addressing non-consensual distribution of intimate images.[260] These statutes provide a civil right of action to those who have had intimate images distributed without their consent. Notably, only half of these laws address morphed or deepfake images and thus could apply to AI generated CSAM.

British Columbia's *Intimate Images Protection Act,* which came into effect on January 29, 2024, was the first to include images that have been "digitally altered" and "AI generated material," including deepfakes, under its definition of "intimate images."[261] Internet intermediaries are not immune from this *Act,* and the *Act's* Regulation provides for administrative penalties against individuals, intermediaries, and other entities should such entities fail to comply with orders made

[260]Those provinces and territories are Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Saskatchewan and Prince Edward Island. *See* Protecting Victims of Non-Consensual Distribution of Intimate Images Act, RSA 2017, c P-26.9); Privacy Act, RSBC 1996, c 373; The Intimate Image Protection Act, CCSM, c 187; Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6; Intimate Images Protection Act, RSNL 2018, c I-22; Intimate Images and Cyber-protection Act, SNS 2017, c 7; Privacy Act, RSS 1978, c P-24; Intimate Images Protection Act, RSPEI 1988, c I-9.1.

[261] Government of British Columbia, Intimate Images and Consent (January 29, 2024). SBC 2023, c 11.

under the legislation.[262] In cases of non-compliance, individuals may face a maximum penalty of $500 per day, up to a total maximum of $10,000 and internet intermediaries or other entities may face a maximum penalty of $5,000 per day, up to a total maximum of $100,000.[263] These penalties are certainly intended to discourage the dissemination of non-consensual intimate images and deepfakes. Manitoba followed suit in June 2024 by adding "fake intimate images created through use of software, machine learning and AI" its existing definition of "intimate images."[264]

Nova Scotia's law, the *Intimate Images and Cyber-Safety Act*, is unique, and among the most comprehensive in that it also covers cyberbullying which is defined broadly as "an electronic communication" that is intended or likely to cause harm to another's health or well-being.[265] The law provides examples of actions that would amount to cyber-bulling including, among other things, communications that are grossly offensive, indecent, or obscene, and communications that amount to criminal harassment and expressly includes AI-generated materials.[266] Successful plaintiffs can be ordered to receive general, special, aggravated, or punitive damages, and can also demand that the intimate image be removed from the internet.[267] Finally, the law in Prince Edward Island defines "intimate image" broadly and explicitly affirms that one may have a reasonable expectation of privacy in an altered image.[268]

To date, courts have not heard cases involving AI-generated images under these provincial laws.

ii. Statutory and Common Law Privacy Torts

The right to privacy is protected under common law torts and privacy legislation in Canada. Some provinces and territories including British Columbia, Saskatchewan, Manitoba, Newfoundland and Labrador, and Quebec have passed personal privacy legislation that broadly prohibits violating the privacy of another and that could be used to seek redress for AI-generated CSAM.[269] For

[262] Intimate Images Protection Regulation BC Reg 293/2023, s 9(1)(a).
[263] Id at s 9(1)(b).
[264] The Intimate Image Protection Amendment Act (Distribution of Fake Intimate Images), S.M. 2024, c. 17, amended C.C.S.M. c. I87 3(1) Subsection 1(1)(a).
[265] Intimate Images and Cyber-protection Act, 2017, c. 7, s. 1.
[266] Id.
[267] Id.
[268] 2020,c.55,s.2; 2020,c.71,s.2.
[269] *See* Privacy Act, RSBC 1996, c 373 s.1 (prohibiting violations of the privacy of another person), s.3 (prohibiting the use of the name or image of another for advertising property or services); Privacy Act, RSS 1978, c P-24 s.2 (prohibiting violations of the privacy of another person), s.3(c) (prohibiting the exploitation of the name, image, or voice of an identifiable person); The Privacy Act, CCSM, c P125. S.2 (prohibiting violations of the privacy of another person), s. 3(c) (prohibiting the exploitation of the name, image, or voice of an identifiable person); Privacy Act, RSNL

example, in the *Civil Code of Québec*, articles 3 and 35 guarantee the right to the integrity of the person and to the respect of privacy, while subparagraph 5 of the first paragraph of article 36 stipulates that the use of a person's name, image, likeness or voice for any purpose other than the information of the public is considered an invasion of privacy.[270] Victims may also avail themselves of the civil liability remedy found in article 1457 of the *Civil Code of Québec* for any injury caused by a deepfake.[271] Similarly, under s. 1(1) of the *BC Privacy Act* "it is a tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another." [272] The remaining provinces and territories do not have personal privacy legislation but victims in those jurisdictions may be able to rely on one or more common law privacy tort theories to seek redress.

Intrusion upon seclusion and public disclosure of private facts are two common law torts that have so far only been recognized in Alberta, Ontario, and Nova Scotia.[273] In general, to succeed on a claim for intrusion upon seclusion the aggrieved must prove a reckless invasion into their private affairs of the kind that a reasonable person would find to be highly offensive and that the intrusion resulted in distress, humiliation, or anguish.[274] Similarly, to establish a claim for public disclosure of private facts the aggrieved must prove publication of an aspect of their private life without consent in a manner that would be highly offensive to a reasonable person in the aggrieved' s position.[275] While provincial courts have not yet dealt with the question of whether individuals have a reasonable expectation of privacy in a digitally altered or AI-generated image of themselves, image-based abuse claims have been successful in Ontario and Alberta.[276]

At present, British Columbia, Saskatchewan, and Newfoundland and Labrador have legislation in place that prohibits the unauthorized use of a person's name, likeness, or personality for financial

1990, c P-22. s. 3 (prohibiting violations the privacy of another person), s. 4(c) (prohibiting the use of the name, image, or voice of an identifiable person or a person's letters, diaries, or other personal documents); Civil Code of Québec, CQLR c CCQ-1991s.35, 36 (prohibiting invading the privacy of another person without their consent or without being authorized by the law).

[270] Civil Code of Québec, CQLR c CCQ-1991s.35, 36

[271] Id at s. 1475.

[272] Privacy Act, [RSBC 1996] Chapter 373.

[273] *See* Carbone v Burnett, 2019 ABQB 98; Jones v Tsige, 2012 ONCA 32; Doucette v. Nova Scotia, 2016 NSSC 25.

[274] Id.

[275] Jane Doe 72511 v. N.M., 2018 ONSC 6607; Racki v Racki, 2021 NSSC 46; EV v Shellington, 2021 ABQB 739 .

[276] Jane Doe 72511 v NM, 2018 ONSC 6607; EV v Shillington, 2021 ABQB 739.

gain.[277] Posting a deepfake image or video on a website that monetizes it in some capacity, including by monetizing traffic through advertisements, could represent a cause of action. This tort could also potentially be used to put more pressure on host websites to take on a more active role in vetting the material uploaded on their platforms.

Finally, courts in Ontario and British Columbia recognize the common law tort of false light as set forth in the American *Restatement Second of Torts*.[278] Since its recognition as an independent tort in 2019, there have been fewer than a handful of decisions based on false light claims, and none within the context of AI-generated images.

iii. Intentional Infliction of Mental Suffering and Harassment Torts

Intentional infliction of mental suffering (IIMS) is another common law tort that may be available to victims of image-based abuse. To prove IIMS, you must show that the defendant intentionally– or with reckless disregard as to the potential to cause emotional distress– engaged in flagrant or outrageous conduct causing plaintiff to suffer a visible and provable illness such as anxiety or depression. [279] In Ontario**,** a claim for IIMS for image-based abuse was successful with a defendant who posted an intimate video of his girlfriend to a pornography website causing her to suffer extreme emotional distress.[280]

The tort of harassment is similar to a claim for IIMS though the test requires only that the plaintiff suffer emotional distress rather than illness, for which the defendant's conduct was a proximate cause.[281] Since this test is a lower bar than the test for IIMS, harassment may be a viable avenue for legal recourse if subsequent case law upholds this tort. The obvious difficulty with respect to both types of claims is proving that the creation of AI-generated CSAM was intended to produce harm rather than having been produced for the creator's pleasure.

---

[277] *See* infra n. 270.
[278] Yenovkian v Gulian, 2019 ONSC 7279; Durkin v Marlan, 2022 BCSC 193.
[279] See e.g., Lu v Shen,2020 BCSC 490.
[280] Id.
[281] In 2017, an Ontario court affirmed the existence of the tort of harassment, which was previously controversial in Canada Merrifield v The Attorney General, 2017 ONSC 1333.

C. REGULATORY FRAMEWORK FOR DEVELOPERS AND ONLINE SERVICE PROVIDERS

In April 2023, the Canadian federal government updated its *2020 Directive on Automated Decision-Making*—part of Canada's broader *Policy on Service and Digital*—to address the risks posed by emerging AI technologies. [282] The Directive outlines administrative obligations for automated decision-making in the absence of binding AI legislation, emphasizing principles such as understanding AI's impact, ensuring transparency, and protecting privacy. [283] It also mandates essential practices, including bias testing and recourse mechanisms to support accountability and fairness. Since then, lawmakers have introduced legislation on AI governance that extends beyond public administration to ensure responsible design and deployment across all systems. Two bills in particular, the *Artificial Intelligence and Data Act* and the *Online Harms Act*, have received widespread bipartisan support.

i. Artificial Intelligence and Data Act

The *Artificial Intelligence and Data Act* ("AIDA"), currently in committee following its second reading at the House of Commons as part III of Bill C-27, is the federal government's answer to the problem of AI under-regulation.[284] It focuses on regulating organizations that develop AI systems and make them available for use by creating Canada-wide obligations and prohibitions pertaining to the design, development and use of AI systems in the course of international or interprovincial trade and commerce.[285] Among these obligations, organizations that develop or make AI systems available for use are required to identify, assess, and mitigate the risk of harm caused by the system. [286] The Act also creates a criminal offense for making an AI system available for use knowing or being reckless as to the fact that it is likely to cause serious physical or psychological harm and where its use actually causes that harm.[287]

---

[282] Government of Canada, Policy on Service and Digital, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603
[283] Id.
[284] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act, 1st Sess, 44th Parl, 2022.
[285] Id.
[286] Id.
[287] Id.

The Act would also criminalize the possession or use of personal information in the design, development, operation, or deployment of AI systems when the individual knows, or should know, that the data was obtained— directly or indirectly—through violations of federal or provincial law.[288] The offense extends to situations involving actions committed abroad that would have constituted a crime if carried out within Canada, ensuring that illegal data use in AI development is penalized, regardless of its origin.[289]

It is unclear how this will apply in practice to the misuse of image generation programs, given their already overwhelming popularity for usually innocuous purposes. However, the obligation to implement risk mitigation measures could require developers to, for instance, require organizations to bias their systems against the production of CSAM.

ii. Online Harms Act

On February 26, 2024, Canadian lawmakers introduced the *Online Harms Act*, a landmark bill designed to enhance online safety, protect children, and hold social media companies accountable for content hosted on their platforms.[290] The Act is also the first piece of federal legislation to explicitly address deepfakes, signaling a new regulatory approach to tackling AI-generated content.

A key focus of the Act is on the protection of children from various forms of harmful online content, including material that sexually victimizes a child and "intimate content communicated without consent."[291] The Act defines "intimate content communicated without consent" broadly, to encompass any visual media—such as photographs, films, or videos—that falsely depicts a person, including through deepfake technology, as being nude, exposing their genitalia, or engaging in explicit sexual activity without their consent.[292]

The Act also establishes the Digital Safety Commission of Canada to enforce compliance, and contribute to the development of regulatory standards, supported by the Digital Safety

[288] Id at Section 38.
[289] Id.
[290] Bill C-63, Online Harms Act, 1st Sess. 44th Parl. (2024).
[291] Id.
[292] Id.

Ombudsperson, who will advocate for public interests and aid those impacted by harmful content.[293]

Finally, the Act will require social media companies to submit digital safety plans, incorporate child protection features into their platforms, and make harmful content inaccessible in Canada. Large platforms are mandated to remove certain types of harmful content, such as child exploitation and non-consensual intimate material, within 24 hours of notification. [294]

Although the *Online Harms Act* is a significant step in the right direction, there is growing consensus on the need for specific but comprehensive legislation to ensure all forms of AI-generated harm are effectively addressed and that digital platforms operate responsibly in the evolving online landscape.

V. DISCUSSION & RECOMMENDATIONS

The primary legal frameworks for addressing CSAM — "child pornography" and obscenity laws—differ significantly across jurisdictions, particularly in their ability to confront the complexities introduced by AI-generated content. In the U.S., the federal CSAM statutes– 18 U.S.C. § 2252A and § 1466A –together with interpretive case law, seek to regulate the evolving threat by criminalizing several categories of harmful material: 1) morphed images depicting identifiable minors, even if no actual minors were involved in the model learning process; 2) computer-generated images that are virtually indistinguishable from an actual minor engaging in sexual conduct; and 3) wholly synthetic depictions of minors engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse.

Despite these protections, significant ambiguities persist. For example, there is a solid constitutional argument under *Ferber* for regulating virtual CSAM as its models are frequently trained on datasets containing real CSAM, thus perpetuating harm to the children depicted, and widespread data scraping activities for model training may drive demand for new CSAM to sustain this pipeline. However, the *Ashcroft* ruling complicates matters by extending First Amendment

[293] Id.
[294] Id.

protections to virtual CSAM unless it meets obscenity standards. This has created a legal gray area that persists, even as the FBI has declared that AI-generated CSAM will be prosecuted with the same severity as traditional CSAM. [295]

Whereas §2252A operates as a strict liability offense, prosecution under §1466A relies on a nuanced, case-by-case analysis under the *Miller* test, which applies inconsistently to AI-generated CSAM that may not meet traditional obscenity criteria. As a result, §2252A has been the statute of choice for prosecution, with §1466A cited in federal court rulings only 133 times in the two decades since the PROTECT Act's passage. [296] That §1446A is rarely invoked is understandable due to the evidentiary burden of proving distribution intent. Prosecutors typically require concrete evidence, such as incriminating communications or attempts to sell or trade material, which has become increasingly more difficult to access with the rise of end-to-end encryption. This challenge is compounded by 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. Additionally, §2252A(3), which criminalizes the promotion and solicitation of materials "capable of being converted into visual depictions," does not clearly apply to AI-generated models, further complicating enforcement efforts.

The challenge of secondary liability also looms large, given the involvement of online service providers in distributing digital content. Drawing on copyright law principles, platforms and developers can be held liable if they knowingly contribute to the dissemination of harmful content. However, §230 of the CDA protects online platforms from civil liability for user-generated content, complicating efforts to hold them accountable for hosting AI-generated CSAM. Reforming §230 has become a focal point for legislators aiming to close this accountability gap, but achieving a balance between platform liability and free speech protections remains a challenge.

At the state level, U.S. laws vary widely in their approach to regulating CSAM. Although at least 39 states and 1 U.S. territory have statutes with language broad enough to reach some forms of AI-generated CSAM, purely synthetic depictions are largely unregulated. Recognizing these gaps,

[295] Federal Bureau of Investigation, Child Sexual Abuse Material Created by Generative AI and Similar Online Tools is Illegal, I-032924-PSA (Mar. 29, 2024), https://www.ic3.gov/PSA/2024/PSA240329
[296] A Westlaw search of §1466A lists 605 citing references total.

several states are updating their statutes to align with federal frameworks, such as the PROTECT Act, which criminalizes morphed imagery and has withstood First Amendment scrutiny. State obscenity laws also differ substantially, with each state defining obscene material according to its own statutes and community standards. These jurisdictional disparities complicate enforcement efforts, as content that is illegal in one state may still be accessible in others. As a result, there is a growing need for harmonized state-level regulations and interstate cooperation to effectively counter the spread of AI-generated CSAM.

In Canada, the federal Criminal Code lacks explicit prohibitions against AI-generated CSAM, although sections 163.1 and 163, as interpreted by the Supreme Court of Canada, provide some coverage by criminalizing the following types of harmful material: 1) sexually explicit morphed images of actual minors; 2) computer-generated images that are indistinguishable from actual minors engaging in sexually explicit conduct; 3)synthetic images that combine sexual content with elements of violence, cruelty, or degradation; 4) visual depictions, audio recordings, and written materials that advocate for or incite criminal sexual activity with a minor; and 5) written materials that describe criminal sexual activity with a minor. However, Canadian courts have read two exceptions to the Code's prohibition on CSAM: material created solely for personal use by the accused and artistic works lacking exploitative intent. These exceptions complicate enforcement efforts and may undermine the law's core objective of preventing harm to children and problematic social attitudes that normalize their exploitation. Furthermore, while the Criminal Code's coverage of CSAM includes visual, written, and audio content that directly harms a child or incites illegal conduct, the law is unclear regarding non-visual materials, such as AI datasets used to produce CSAM.

Canadian federal law also criminalizes the non-consensual distribution of intimate images under section 162.1 of the Criminal Code, though the application of these provisions to AI-generated CSAM, including deepfakes and morphed images, remains uncertain. Enforcement falls to provincial agencies, and civil remedies for victims vary widely across provinces, creating a patchwork of protections where access to relief depends on the victim's location or the jurisdiction where the unauthorized use occurred. Although Canada does not have an equivalent to §230 of the CDA, the country still faces challenges in holding tech companies accountable for user-generated content, as Canadian law provides limited means to penalize platforms knowingly hosting or

distributing CSAM. In the absence of regulations targeting the safe development of generative AI tools or laws prohibiting their misuse, online service providers and developers are mainly able to avoid liability by shifting exclusive blame onto users who engage in abusive applications of their technologies.

Privacy laws in both the U.S. and Canada offer some avenues for recourse, but they often fail to capture the specific harms associated with AI-generated CSAM. Privacy torts often require elements like commercial use, verifiable falsehoods, or physical intrusion, which are frequently absent in synthetic imagery cases. Existing non-consensual distribution of intimate images laws also fall short, as they generally require intent to harass or coerce, a standard that may not align with cases where AI-generated content is created purely for personal gratification, often with no intent for the victim to discover the material. Ambiguities in statutory language further complicate enforcement efforts. For example, many laws require that the individual depicted appear "nude" or engaged in "sexual conduct." While deepfake images often depict individuals "as" nude, the underlying image may not contain explicit content. Statutes also typically cover images recorded in situations that imply a reasonable expectation of privacy, a requirement that can be challenging for cases involving public photos that are manipulated into deepfakes.

Copyright law offers a potential, though complex, avenue for addressing AI-generated CSAM. Copyright protections in both countries cover original works, granting creators exclusive rights over their reproduction and distribution, which could extend to individuals whose public photos are used to train AI models or incorporated into synthetic CSAM. Victims may seek redress through copyright infringement claims or removal mechanisms like the Digital Millennium Copyright Act (DMCA) in the U.S. and equivalent Canadian laws. However, copyright law's application to synthetic CSAM is complicated by exemptions for personal use and non-commercial content, which offenders may invoke if the material remains private, while courts must also grapple with whether deepfake images qualify as artistic expression under fair use. Moreover, online platforms hosting AI-generated CSAM typically avoid direct liability unless they knowingly facilitate infringement, adding another layer of complexity to enforcement.

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* and *Sharpe* 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 modernize 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 modern 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, and related provisions in Canada's Criminal Code, 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 criminalizes 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, Section 163.1 of Canada's Criminal Code and 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. and Canadian "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 CSA, 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 criminalize 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 criminalizing 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: Amend CSAM Statutes to Cover Content that is Legal but that Poses a Substantial Risk of Harm to Minors

Courts in the United States and Canada recognize that an image need not depict the physical sexual abuse of a child for it to be the product of sexual exploitation. Indeed, even material that is not illegal can and does play a role in the offending cycle. Even images that may not be inherently abusive raise important questions regarding the role of consent particularly in today's digital world where any image is "primed for entry into the distribution chain" of underground child predators.[297] Several types of harmful content evade criminal classification yet require regulation to effectively protect minors. Key examples include:

1. **Visual Content**:

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

- Images of minors in states of nudity or partial nudity, captured or distributed with intent to sexualize or exploit.
- Photos, videos, or digital images of children in fetishistic or exploitative contexts, including under the guise of "child modeling."
- Visual depictions of abuse-related events, including moments leading up to, during, or after an abusive act.
- Photos of children in swimwear or everyday clothing shared on forums that fetishize minors.

2. **Grooming-Related Content**:
    - Materials or communications that promote, facilitate, or normalize grooming behavior.
3. **Sexualized Commentary or Discussion**:
    - Textual content that glorifies, promotes, or describes child sexual abuse.

To address these gaps, both countries need to adopt broader definitions that capture harmful content, even if it does not meet the strict criminal definition of CSAM. An expanded definition could classify 'child abuse material' as any content involving or depicting minors that is reasonably likely to cause harm, exploitation, or psychological distress, regardless of whether it meets the criminal standard for CSAM.

Recommendation #4: Establish a Legally Binding Framework for Safe and Responsible AI Development and Deployment

Effective AI governance requires the establishment of a dedicated regulatory agency tasked with overseeing the development and deployment of generative AI and similar technologies. This agency should have the legal authority to impose criminal and civil penalties for non-compliance with regulatory standards and ensure adherence to robust child protection measures across the industry.

To prioritize child safety, the agency should enforce a duty of care, obligating developers and online service providers to adhere to defined operational standards. These standards should 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 blocking IP addresses linked to anonymized services such as Tor, filtering search terms associated with CSAM, and suspending accounts distributing abusive content.

Finally, the agency should enforce strict liability for developers and platforms that fail to vet their datasets or adequately monitor AI outputs, imposing financial penalties proportional to the volume, severity, and delayed removal of harmful content. Such a framework would promote accountability and ensure that AI technologies are developed and deployed responsibly, prioritizing child safety at every stage.

Recommendation #5: Expand Legal Protections to Include Control Over One's Own Image

The U.S. and Canada 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, unauthorized 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 unauthorized 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 unauthorized 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.

VI. CONCLUSION

While existing CSAM laws in the U.S. and Canada 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. Both countries 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.

The recommendations outlined in this report underscore the urgent need for targeted reforms. These include updating statutory definitions to encompass AI-generated CSAM and the misuse of AI technologies and expanding liability for developers and service providers that facilitate this form of child exploitation and abuse. By also addressing broader forms of harmful content and

enhancing civil remedies, these reforms aim to strengthen protections for children while establishing a clear framework for accountability within the AI ecosystem.

Ultimately, effective regulation will require a coordinated approach across federal, state, and provincial jurisdictions, coupled with international collaboration to close regulatory loopholes that offenders and businesses alike continue to exploit. Both the U.S. and Canada have the opportunity to pioneer comprehensive AI governance standards that protect vulnerable populations while balancing innovation with ethical responsibility. Establishing these protections will not only help deter misuse but also affirm a commitment to child safety and public trust as AI technologies continue to evolve.