

Pennsylvania's Legislative Gaps in Protecting Minors from Deepfake-CSAM Exploitation

By Anosh Matti

Founder, Matti Deepfake Advisory LLC

This policy brief is adapted from original graduate research completed for my Master of Public Policy capstone at Drexel University, including structured interviews with three Pennsylvania state legislators — Senator Tracy Pennycuik, Representative Robert Merski, and Senator Lisa Boscola — conducted in 2025. It has been lightly edited from its original academic form for publication.

Introduction

Deepfake technology now makes it possible to take a photograph of a real person's face and generate a fabricated, sexually explicit image of them, without their knowledge or consent. When the subject is a minor, that output is child sexual abuse material (CSAM), regardless of whether any physical contact ever occurred. This is not a hypothetical risk: it is an increasingly routine occurrence in schools, workplaces, and online communities.

This case study examines the rapid emergence of AI-generated CSAM ("deepfake-CSAM") and the unique challenges it poses for law, schools, and law enforcement. Pennsylvania has acted more quickly than most states to update its statutory framework, particularly through Senate Bill 1213, enacted as Act 125 of 2024, yet the real-world implementation of these laws continues to lag the pace of technological change. This paper argues that Pennsylvania has built a comparatively strong legal architecture to confront deepfake-CSAM, but institutional culture, reporting practices, and enforcement capacity remain out of step with legislative innovation. By examining Pennsylvania's major deepfake incidents and tracing how law, scandal, and enforcement interact, this study maps the friction points between statutory progress and institutional practice — and shows how the promise of legal protection for minors can go unrealized without meaningful implementation.

Two Pennsylvania Incidents

Pennsylvania's experience with deepfake exploitation first drew national attention in 2021, when a Bucks County mother, Raffaella Spone, was accused of using low-cost deepfake tools to fabricate images of her daughter's cheerleading teammates appearing naked, drinking, or smoking, allegedly in an effort to have those girls removed from the squad. Although the case proved more complex than early reporting suggested, it was a cultural inflection point: it showed that ordinary individuals, not just technical specialists, could weaponize synthetic imagery against minors. Prosecutors, lacking statutes tailored to synthetic CSAM at the time, relied on general harassment and child-endangerment laws — exposing a real gap in the legal framework.

By 2023–2024, the stakes escalated further. At Lancaster Country Day School, a group of students used publicly available photos of classmates — pulled from Instagram or the school website — to generate AI-fabricated nude images, which then circulated through group chats. The school had received an anonymous Safe2Say tip nearly a year before parents discovered what had happened, but the tip was never escalated. The resulting delay triggered student walkouts, parental outrage, leadership resignations, and a criminal investigation.

Together, these cases illustrate two recurring themes: deepfake technology causes profound psychological harm — fear, humiliation, loss of bodily autonomy — even without physical contact; and institutions are frequently unsure how to classify synthetic images (as misconduct, bullying, or child abuse), which produces hesitation and inconsistent responses.

More recently, publicly accessible generative AI tools have lowered the barrier to entry further still, making it possible to produce sexualized synthetic images of real people from a single uploaded photo and a simple text prompt. This ease of use means many victims never receive justice: platforms struggle to trace who generated an image, whether it is AI-generated at all, or what real photo was used as its source, and perpetrators can distribute the results widely with little practical risk of detection. These incidents are not isolated events — they are analytical anchors for understanding how Pennsylvania's laws interact with institutional behavior.

It is worth being clear-eyed about the limits here. Even where content is flagged or watermarked, a large volume of deepfake-CSAM goes undetected, and current law enforcement tools cannot reliably determine whether an image is AI-generated or trace it back to its source photo or creator. Legislators can and do classify this content as CSAM for prosecutorial purposes, but no legal framework can fully close the gap between the pace of generative-AI misuse and the pace of detection technology.

Pennsylvania's Legislative Response

The urgency of regulating deepfake exploitation became clear in the aftermath of these incidents. Pennsylvania responded with a series of statutory efforts. As part of this research, I interviewed three state legislators: Senator Tracy Pennycuick, Representative Robert Merski, and Senator Lisa Boscola. The interviews were conducted over Zoom in mid-2025. Senator Pennycuick was the prime sponsor of Senate Bills 1213 and 1050; Senator Boscola co-sponsored both. Representative Merski co-sponsors House Bill 1598, an Unfair Trade Practices and Consumer Protection Law amendment that would ban distribution of AI-CSAM; like SB 1050, it has not yet been signed into law. HB 1598 was referred to the Communications and Technology Committee in April 2024 and has not moved further.

In my interview with Senator Pennycuick, she described a prior “loophole” in which prosecutors lacked explicit authority to charge perpetrators for synthetic images depicting minors. Senate Bill 1213, signed into law in October 2024 as Act 125, closed that loophole by making the creation and distribution of AI-generated or manipulated sexual images of minors a criminal offense, and by replacing the term “child pornography” with “child sexual abuse material (CSAM)” to align state terminology with federal standards. The statute defines an “artificially generated sexual depiction” as a visual depiction that

appears to authentically show an individual in a state of nudity or engaged in sexual conduct that did not occur in reality, and whose production was substantially dependent on technical means (Act 125 of 2024, § 4, p. 4). Contemporary reporting on the law confirmed that it specifically targets deepfake sexual exploitation and enhances penalties involving minors, ensuring synthetic imagery falls squarely within CSAM statutes.

Representative Merski's legislative focus is broader, covering AI voice impersonation and digital deception generally. In our interview, he also described Pennsylvania's Task Force on AI, which includes academic experts alongside legislators — a sign that the state is trying to build institutional expertise, not just pass statutes. He argued that some uses of AI “should be out of bounds,” suggesting support for bright-line prohibitions rather than case-by-case judgment calls.

Senate Bill 1050 strengthens mandated-reporter requirements, clarifying that AI-generated intimate images of minors must be reported as potential child abuse, and that any intimidation, retaliation, or obstruction of such a report is independently punishable under existing child-abuse-reporting law (SB 1050, p. 3). This provision responds directly to what happened at Lancaster, where school administrators hesitated to escalate synthetic images to law enforcement. The bill passed the Senate and was sent to the House Judiciary Committee in November 2025, where it remains — unsurprising, given that it amends Title 23 (Domestic Relations) child-protection provisions, which typically move more slowly and carry more deliberation than SB 1213 did.

Senator Boscola summarized the intent behind these bills directly in our interview:

“High school is hard enough with social media. Now you add the ability to embarrass someone forever by posting a fake image — something needed to be done.”

Together, these bills show Pennsylvania moving deliberately to modernize its Crimes Code for an era of AI-enabled exploitation, extending existing cyberbullying and child-protection concerns to cover synthetic media specifically.

Where Strong Law Meets Weak Enforcement

If Pennsylvania's legal framework is comparatively strong, why did the Lancaster case still take months to surface? Interviews and secondary research point to enforcement and institutional practice as the real choke points. Mandated reporters often hesitate; schools frequently treat deepfake images as disciplinary matters rather than potential crimes, handling them internally instead of escalating them. Local police commonly lack the digital-forensics training and tools needed to move quickly. Prosecutors face genuine uncertainty about whether synthetic images of fictional (rather than real, identifiable) minors are chargeable. And after the contested Bucks County case, some institutions grew more cautious about moving quickly on AI-related accusations at all.

Senator Pennycuik emphasized, in our interview, the gap between the number of cases actually charged and the true volume of AI-CSAM in circulation. Without consistent reporting and enforcement, even a strong statutory framework cannot realize its protective potential. The Lancaster case illustrates

this enforcement lag starkly: despite Act 125 being in effect, school officials did not escalate an anonymous tip, leaving affected students unprotected for nearly a year.

At the federal level, the TAKE IT DOWN Act (Pub. L. No. 119-12, signed May 19, 2025) criminalizes the publication or threatened publication of non-consensual intimate images, including deepfakes, and requires covered platforms to remove flagged content within 48 hours of notice. This establishes a federal notice-and-takedown baseline, but it does not mandate watermarking, provenance tracking, or any proactive detection technology — it is a response mechanism, not a prevention one.

How Pennsylvania Compares

Legislation	Status / Jurisdiction	Primary Purpose	Connection to Enforcement Gap
Act 125 of 2024 (SB 1213)	Law — Pennsylvania	Criminalizes creation and distribution of AI-generated sexual images of minors; replaced “child pornography” with “CSAM.”	Closes the prosecutorial loophole, ensuring AI-CSAM is clearly chargeable.
Senate Bill 1050	Proposed — Pennsylvania	Strengthens mandated-reporter requirements for AI-generated intimate images.	Targets the institutional gap by forcing schools/reporters to escalate synthetic images to law enforcement immediately.
TAKE IT DOWN Act (Pub. L. 119-12)	Law — Federal	Criminalizes publication/threatened publication of non-consensual intimate images; requires platform takedown.	Federal notice-and-takedown baseline; no criminal mechanism for content removal.
California AB 2655, 2839, 2355	Laws — California	AI governance covering transparency, political-ad disclosure, and performer protection from unauthorized digital replicas.	Contrasts with PA's criminalization-heavy approach; highlights PA's blind spots in provenance and civil remedies.
Executive Order 2023-19	Executive Order — Pennsylvania	Establishes governance for generative AI use within Commonwealth government agencies.	Shows the state's broader interest in regulating AI, but does not directly address deepfake-CSAM enforcement.

California's model emphasizes transparency and platform responsibility; Pennsylvania's emphasizes criminalization and minor-focused CSAM statutes. Pennsylvania is a national leader on synthetic-CSAM criminalization, but it lacks transparency mandates, provenance or watermarking requirements, and civil remedies comparable to California's.

Case-study scholarship (notably Flyvbjerg, 2006) argues that case studies offer practical, context-dependent knowledge that reveals how power actually operates within institutions. Pennsylvania is a useful case precisely because it has explicit deepfake-CSAM law, has experienced multiple school-based incidents, and is operating within a national moment of AI-focused legislative activity. Read alongside legislative timelines, task-force deliberations, and enforcement hearings, a mechanism emerges: scandal catalyzes legislation, but enforcement lags behind it, and children fall into the resulting gap.

A fair counterargument, drawing on Jensen and Rodgers' emphasis on interrogating alternative explanations, is that schools and prosecutors are not so much “failing” as being cautious in the face of

legal ambiguity and civil-liberties concerns — particularly after the contested Bucks County case. This does not contradict the paper's central argument so much as complicate it: enforcement gaps arise from the interaction of ambiguity, institutional caution, and rapid technological change, not from any single failure.

Recommendations

No jurisdiction — Pennsylvania included — can fully guarantee protection against deepfake-CSAM given the current state of detection technology; even tools that claim to identify AI-generated content are not reliably accurate, and tracing a synthetic image back to its source photo or creator remains genuinely difficult. Legislation cannot close that technical gap on its own. What it can do is ensure that everyone — schools, families, law enforcement — has a clear protocol to follow when an incident occurs. Based on this research, four areas stand out:

Standardized statewide protocols. SB 1050 should be paired with mandatory statewide procedures requiring immediate Safe2Say and law-enforcement notification, digital-evidence preservation, parent communication, and trauma-informed victim support — removing the discretion that allowed the Lancaster tip to sit unescalated for a year.

Digital forensics capacity. State funding should support image-authenticity analysis tools, training for police and prosecutors, and dedicated platform-liaison units, so that investigations do not stall for lack of technical capability.

Legislative refinement. Pennsylvania could explicitly criminalize synthetic depictions of fictional minors, closing off a potential “no real child was harmed” defense, and strengthen civil remedies available to minors and their families.

Data and transparency requirements. Annual public reporting on AI-CSAM referrals and charges would let lawmakers actually measure whether these statutes are working, rather than relying on anecdote.

To illustrate what this would have meant in practice: had SB 1050's mandatory-reporting requirements, standardized protocols, and forensic capacity already existed at the time of the Lancaster incident, the initial anonymous Safe2Say tip would have been legally required to reach county child-welfare officials and police within hours rather than months. Trained investigators with authenticity-triage tools could have preserved digital evidence before wider distribution, and counseling and school protections could have been activated immediately — instead of after a year of internal confusion.

A Note on Federal Preemption

Having reviewed legislation at the Pennsylvania, California, and federal levels, my own assessment is that federal action offers the most workable long-term path for AI-CSAM regulation specifically — states will still reasonably legislate around issues like elections and celebrity likeness on their own, but a single federal standard for handling AI-CSAM cases (including consistent platform obligations) would prevent

perpetrators from exploiting inconsistencies between state laws, particularly in cases that cross state lines. This is a personal policy judgment rather than a finding compelled by the research itself, and reasonable people, including some of the legislators I interviewed, disagree — there are legitimate federalism and enforcement-capacity arguments for leaving more of this to the states.

A Note on Juvenile Offenders

One further judgment call worth stating plainly, separate from the descriptive findings above: at Lancaster, the students who generated the images were themselves minors, not adult predators. I do not believe it follows that they should face identical criminal charges, or juvenile detention, as an adult who deliberately produces CSAM. Some form of accountability is clearly warranted — comparable, perhaps, to how schools handle a student found to have taken inappropriate images of a classmate without consent — but non-criminal sanctions for juvenile offenders using tools they may not fully understand the implications of seems more proportionate than a criminal record. This is a normative recommendation, not a legal finding, and I want to be transparent that it reflects my own view rather than a consensus position among the legislators interviewed for this research.

Legal Exposure Under the Current Framework

The updated statutory landscape — Act 125, SB 1213, SB 1050, and related statutes — creates a dual pathway: criminal liability for perpetrators, and civil liability for institutions or third parties who fail to act. Act 125 directly criminalizes AI-generated or manipulated images of minors, with likely charges including sexual abuse of children, unlawful dissemination of intimate images, criminal use of a communication facility, and corruption of minors. A 2024 Department of Justice prosecution in Harrisburg confirms that AI-generated CSAM, even where fully synthetic, is being actively charged under existing federal frameworks. Under Title 23, mandated reporters who fail to report suspected abuse — including AI-generated images — can face both criminal penalties and civil liability, including claims for negligent supervision, failure to report child abuse, negligent infliction of emotional distress, and breach of duty of care to minors. Parents at Lancaster raised exactly this concern about the school's year-long delay.

Platform-level enforcement remains more limited. Under the TAKE IT DOWN Act, platforms may face regulatory action for failing to remove flagged content, but Section 230 shields remain broad absent further Congressional exceptions, and First Amendment considerations continue to shape how aggressively lawmakers can restrict content creation and distribution generally. A mandatory AI-content watermark — similar to the labels some platforms, including TikTok, already apply automatically to AI-generated video — would likely be only partially effective, since a determined perpetrator could simply strip the label before distributing the content.

Conclusion

Pennsylvania has taken meaningful steps to update its legal framework for deepfake-generated CSAM, culminating in Act 125 of 2024 and the advancement of SB 1050. But statutory innovation alone cannot ensure minors are protected. The Bucks County and Lancaster incidents show that the greatest risk lies

not in legislative gaps but in the space between law and implementation: schools hesitate because synthetic imagery blurs the line between bullying, misconduct, and criminal abuse; mandated reporters are unsure when an AI-generated image constitutes suspected exploitation; and law enforcement often lacks the digital-forensics capacity to authenticate synthetic content quickly.

Pennsylvania is a national leader in criminalizing synthetic CSAM, but that leadership will only translate into real protection if legal reform is matched by standardized reporting protocols, clearer administrative guidance, trauma-informed training, and investment in AI-specific forensic tools. Other states confronting the same challenge can draw a clear lesson from Pennsylvania's experience: modernized law must be matched by operational clarity and technologically competent enforcement. Without that alignment, legislation will continue to outpace the capacity of schools, police, and prosecutors to act on it — leaving minors exposed in precisely the moments the law is meant to protect them.

Selected Sources

- Pennsylvania General Assembly. *Act 125 of 2024 (Senate Bill 1213)*. 2024. legis.state.pa.us
- Pennsylvania General Assembly. *Senate Bill 1050*, Printer's No. 1599, 2025–2026 Session. legis.state.pa.us
- Shapiro, Josh. *Executive Order 2023-19: Building a Responsible Generative Artificial Intelligence Program in the Commonwealth of Pennsylvania*. 2023. pa.gov
- Mekeel, David. "AI-Generated Nude Images of Girls at Lancaster Country Day School Prompt Protests." *Reading Eagle*, 2024.
- Holmes, Kristin. "Mother Accused of Making Deepfake Videos to Harass Daughter's Rivals." *The Philadelphia Inquirer*, 14 Mar. 2021.
- Levy, Marc. "Pennsylvania Passes Bill Targeting Deepfake Sexual Images." *Associated Press*, 2024.
- U.S. Department of Justice. "Harrisburg Man Sentenced for Possessing AI-Generated Child Sexual Abuse Material." [Justice.gov](https://justice.gov), 2024.
- U.S. Congress. *TAKE IT DOWN Act*, Pub. L. No. 119-12, 19 May 2025. congress.gov/bill/119th-congress/senate-bill/146
- California Legislature. AB-2655 (Elections: Deceptive Media); AB-2839 (Political Advertising: AI Disclosure); AB-2355 (Digital Replicas: Protection of Performers). 2024. [leginfo.legislature.ca.gov](https://leginfo.ca.gov)
- Flyvbjerg, Bent. "Five Misunderstandings About Case-Study Research." *Qualitative Inquiry*, vol. 12, no. 2, 2006, pp. 219–245.
- Jensen, Jennifer L., and Laurie Rodgers. *Qualitative Research Methods for Public Policy*. M.E. Sharpe, 2001.
- Pennycuik, Tracy; Merski, Robert; Boscola, Lisa. Personal interviews conducted by the author, 2025.

This research was originally completed as a capstone project for the Master of Public Policy program at Drexel University. Reproduction or redistribution of this document, in whole or in part, without written permission from the author is prohibited.

© 2026 Anosh Matti / Matti Deepfake Advisory LLC. All rights reserved.