

When Fake Images Cause Real Harm

The Legal & Regulatory Frameworks for Addressing AI-Generated CSAM

Presented By Jessica Schidlow, ESQ.



ACE's Health Champions Gathering March 27, 2025



Overview: AI - Generated CSAM

AI is overpowering efforts to catch child predators, experts warn

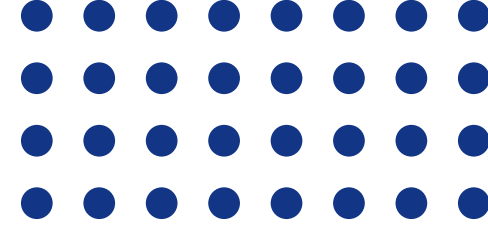
Safety groups say images are so lifelike that it can be hard to see if real children were subject to harms in production



© A single AI model can generate tens of thousands of new images in a short amount of time, flooding the internet. Composite: The Guardian/Getty Images

- AI-Generated CSAM
 - “Deepfake images”
 - Virtual/synthetic CSAM
- How are perpetrators using AI to create CSAM?
 - Text-to-image base models
 - Open-source models
 - Fine-tuned models
 - Alternative methods i.e. “hudifying” apps

Prevalence



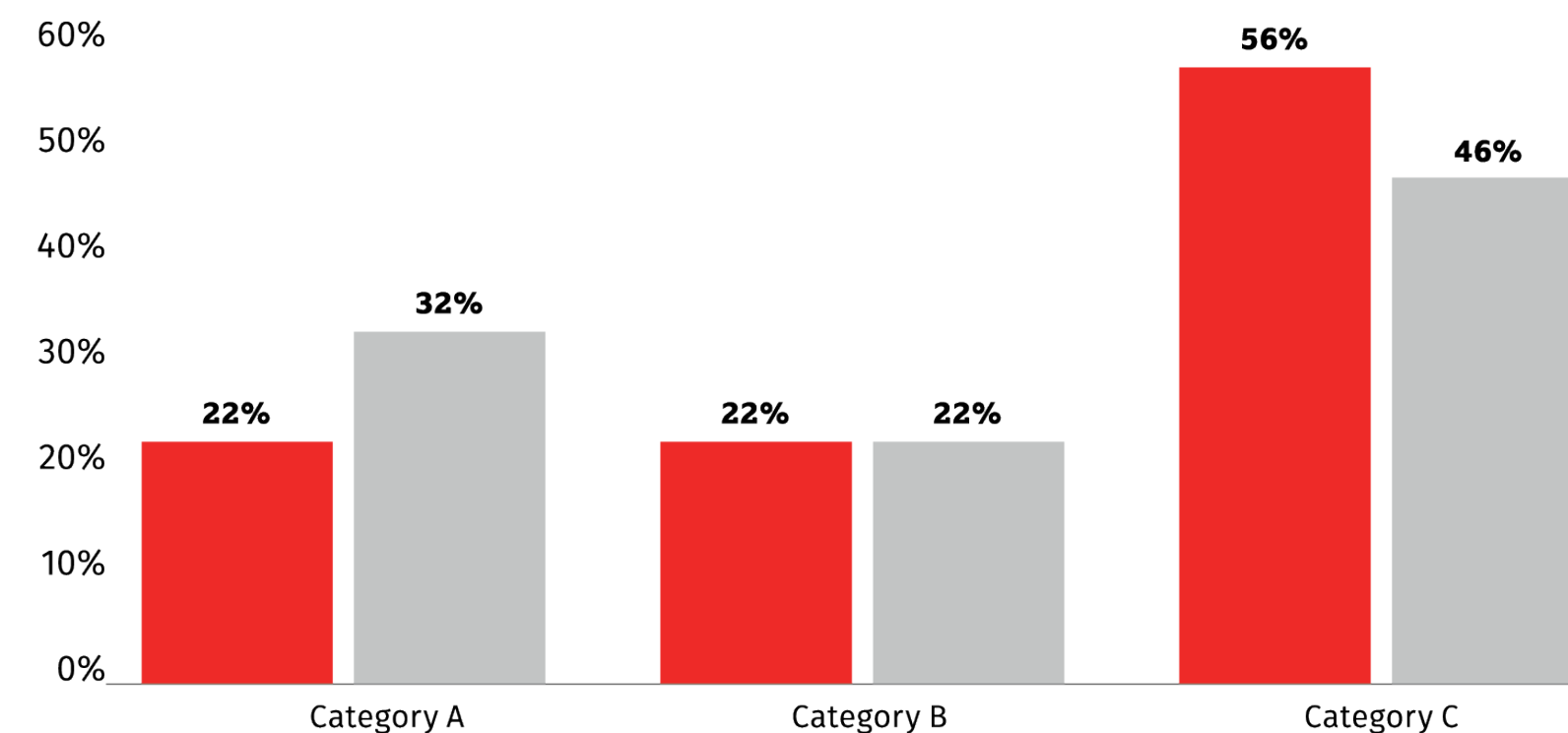
1 in 10



number of children aware of peers using gen-AI to create non-consensual intimate images of others

AI CSAM (pseudo) images by severity

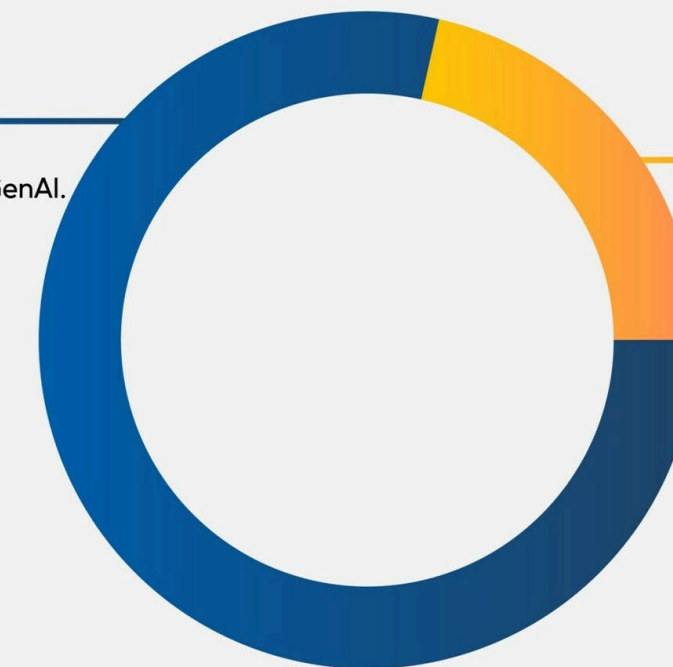
● September 2023 ● March - April 2024



ActiveFence identified a poll of almost 3,000 predators on a closed dark web forum indicating their use of Generative AI.

78.5%

have used or are considering using GenAI.

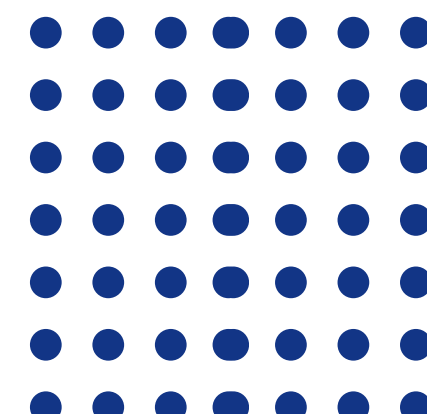


21.5%

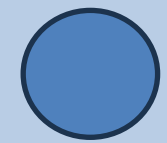
are not interested in, or cannot access GenAI.

4,700

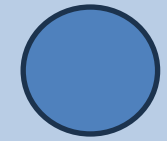
reports of
AI CSAM to the
CYberTipline
in 2023



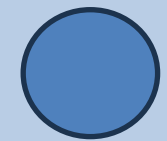
Impact



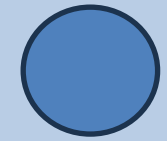
Strains resources and impedes law enforcement efforts



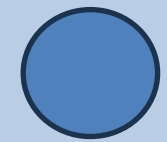
Revictimization of past CSAM targets & creation of new CSAM from benign images



Scalability of grooming/sexual extortion schemes



Normalizes sexualization of children

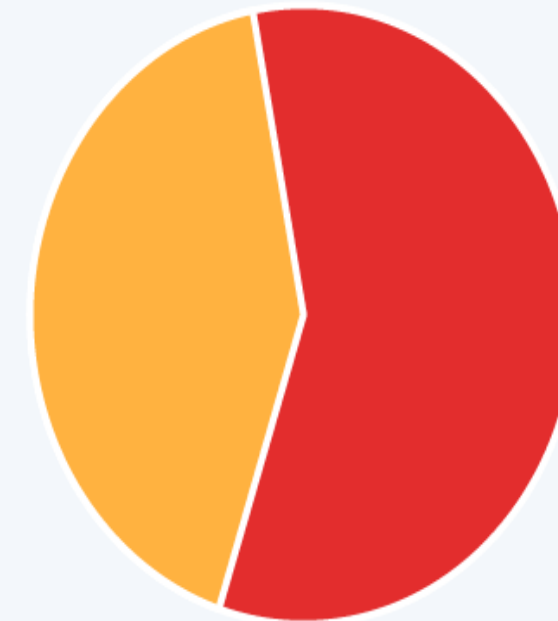


Global effects of victimization on the target and society

Consumption of AI-CSAM content correlates with seeking direct contact with children

42%

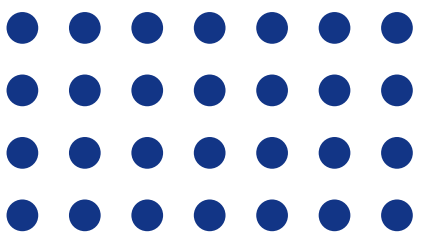
admitted to having sought direct contact with children through online platforms after viewing CSAM



58%

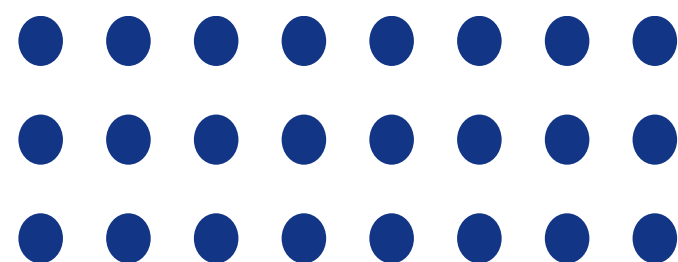
claimed they were afraid their use of CSAM would lead to further sexual acts with a child or an adult

an Lapsia, Protect Children - Tech Platforms Used by Online Child Sexual Abuse Offenders



POLL QUESTION #1

How confident are you in the existing research and evidence-based practices to address the psychological impact of AI-generated CSAM and other forms of digital harm?



Overview Federal Framework

- Landmark U.S. Supreme Court Cases:
 - *Miller v. California*
 - 3-part test for “obscenity”
 - *New York v. Ferber*
 - No First Amendment protection for “child pornography”
 - *Ashcroft v. Free Speech Coalition*
 - adults “appearing” to be minors and CG images beyond the reach of Ferber
- Congressional Response:
 - PROTECT Act (2003)
 - expanded definition of “child pornography” to include CG images that are “indistinguishable” from actual minors
 - pandering provision prohibiting advertising/distribution of material that is not but appears to be “child pornography”
 - *United States v. Williams*



A photograph of a classical building's roofline featuring a statue of Lady Justice holding scales. The image is partially obscured by a white diagonal line on the right side.

Key Federal Statutes

- 18 U.S.C. § 2252A
 - Prohibits possession, production, receipt, and distribution of “child pornography”
- 18 U.S.C. § 1466A
 - Prohibits production, receipt, and possession of obscene visual depictions involving minors
 - Does *not* require that the minor depicted actually exist

State Statutory Framework

At least **39 states and 1 U.S. territory** have “child pornography” statutes broad enough to potentially cover AI-generated CSAM.

Morphed & Synthetic CSAM

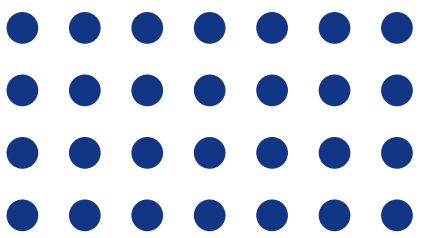
15 states explicitly prohibit morphed images and synthetic images if sufficiently realistic.

Morphed Images Only

14 states & 1 territory expressly prohibit morphed images involving *actual* children but stop short of regulating synthetic content.

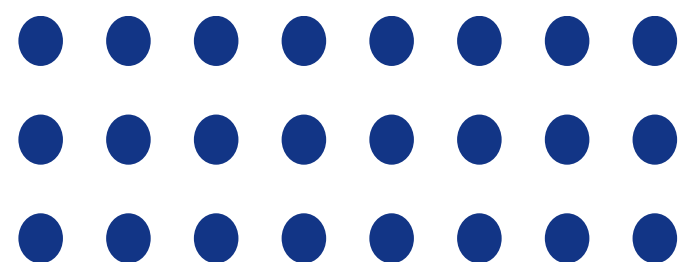
Neither

13 states & 4 territories do not appear to criminalize AI-generated CSAM at all.



POLL QUESTION #2

ARE YOU AWARE OF THE SPECIFIC
LEGAL FRAMEWORKS THAT GOVERN
AI-GENERATED CSAM IN YOUR
JURISDICTION?



Regulatory Framework for Developers & ISPs

- **PROTECT/REPORT Acts**
 - require ISPs to make reports to the CyberTipline
 - only applies to violations under §2252A *not* §1466A
- **Communications Decency Act (CDA) §230**
 - limited defense from liability for third-party content
- **TVPRA/FOSTASESTA**
- Recent cases question whether there is a §230 defense to claims based on gen-AI outputs
- **Proposed Legislation :**
 - EARN IT Act
 - STOP CSAM Act
 - KOSA



Alternative Avenues for Liability



- Nonconsensual distribution of intimate images (NDII)
 - “Deepfake” regulation
 - “Revenge porn” statutes
 - Statutory and common law privacy torts
- Copyright Law
 - Morphed images that incorporate copyrighted material
- Consumer Protection Laws
 - FTC has affirmed that AI technologies are not exempt from oversight
- Proposed Federal Legislation:
 - No AI FRAUD Act
 - NO FAKES Act
 - DEFIANCE Act

State Privacy Laws

- At least **9 states and 1 territory** recognize false light as a distinct privacy tort
- **37 states** recognize the right of publicity
- Courts apply principles of aiding and abetting liability with some states limiting liability for ISPs with knowledge of unauthorized use
- First Amendment challenges involving right of publicity claims in the context of AI:
 - *Anderson v. Stability AI, Ltd.*
 - *In re: Clearview*



State “Deepfake” Laws

49 states &
3 territories
criminalize
nonconsensual
sexual
deepfakes

30 states
criminalize
distribution of
nonconsensual
sexual
deepfakes

22 states
criminalize
distribution with
intent to harm or
with knowledge of
lack of consent

19 states
specifically
prohibit the
creation of AI-
generated
CSAM

11 states
prohibit creation
and distribution
including AI-
generated
CSAM



AI Governance & Accountability

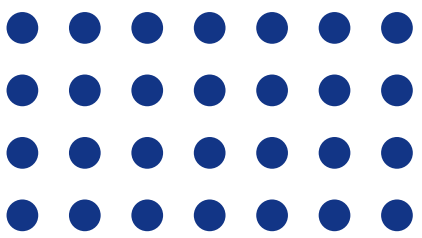


Federal Actions:

- National Artificial Intelligence Initiative Act of 2020
- Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI

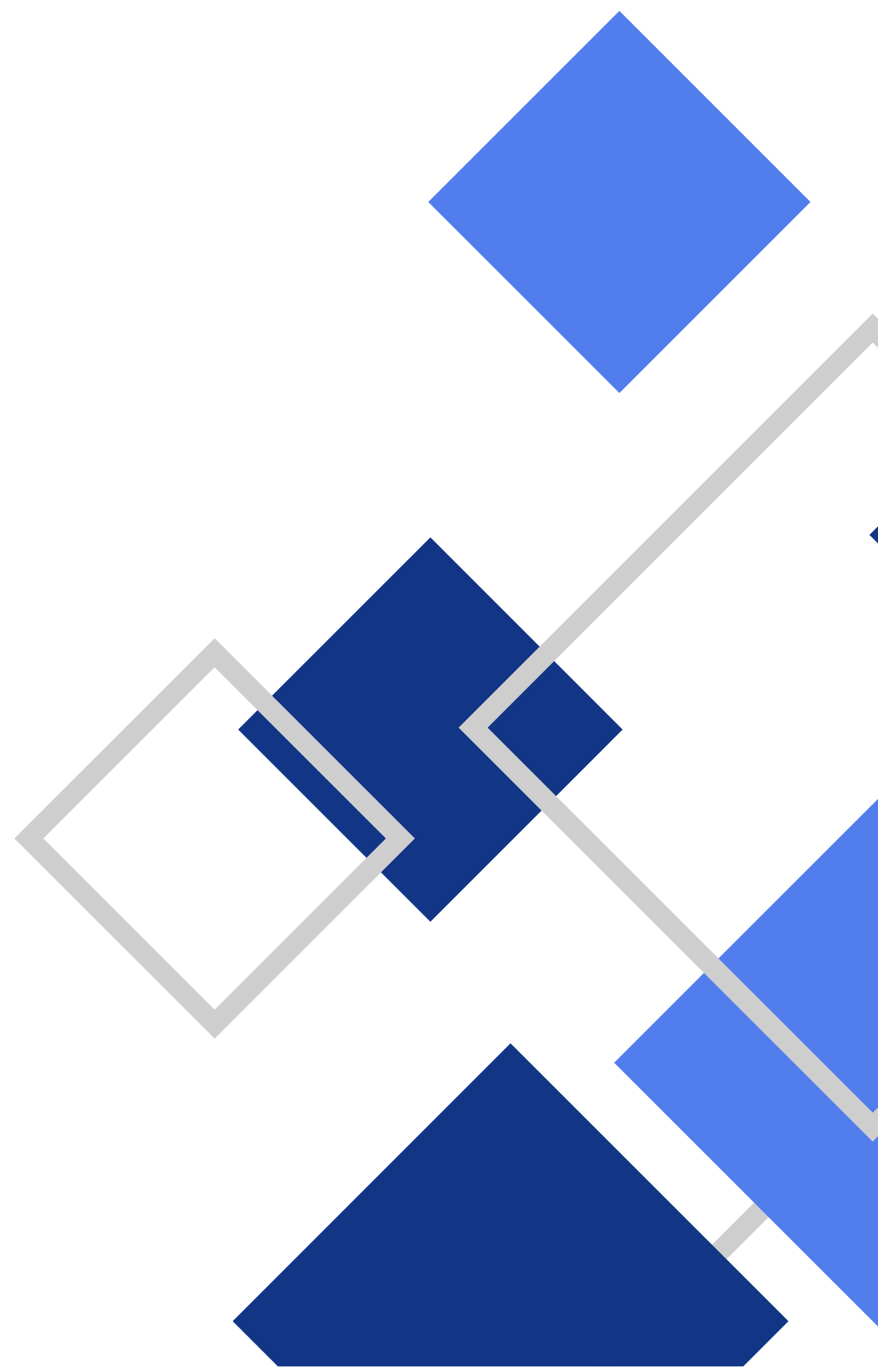
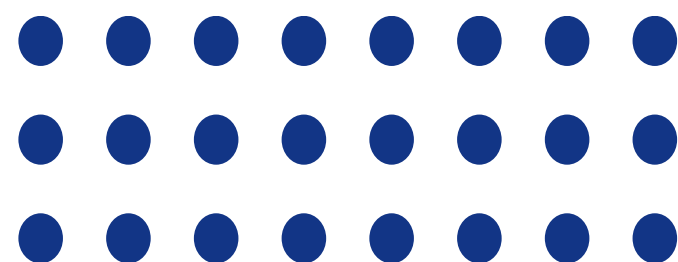
State Actions:

- More than **31 states and 2 territories** passed laws/resolutions focused on regulating the design, development, and deployment of AI systems
- At least **12 states** have formed oversight groups to assess AI's impact on consumers
- Another **12 states** passed laws to hold developers/deployers accountable for non-compliance with AI regulations



POLL QUESTION #3

WHO SHOULD BE PRIMARILY
RESPONSIBLE FOR ADDRESSING THE
ISSUE OF AI-GENERATED CSAM?





Recommendations

1

Amend Existing CSAM Laws to Explicitly Cover AI-Generated Content

2

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

3

Amend CSAM Laws to Cover Content that is Legal but Poses a Substantial Risk of Harm to Minors

4

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

5

Expand Legal Protections to Include Control Over One's Own Image





Governance

Establish clear policies and guidelines for GAI development and deployment, ensuring ethical and responsible use.



Mapping

Identify potential risks and vulnerabilities across the AI lifecycle, from development to decommission.



Measurement

Implement metrics and benchmarks to assess the effectiveness of risk mitigation strategies.



Management

Develop robust mechanisms for monitoring, detecting, and responding to GAI-related risks in real-time.



Q&A

If you have any questions or would like to discuss further, please feel free to reach out.

jschidlow@childusa.org



“Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks.”

-Stephen Hawking