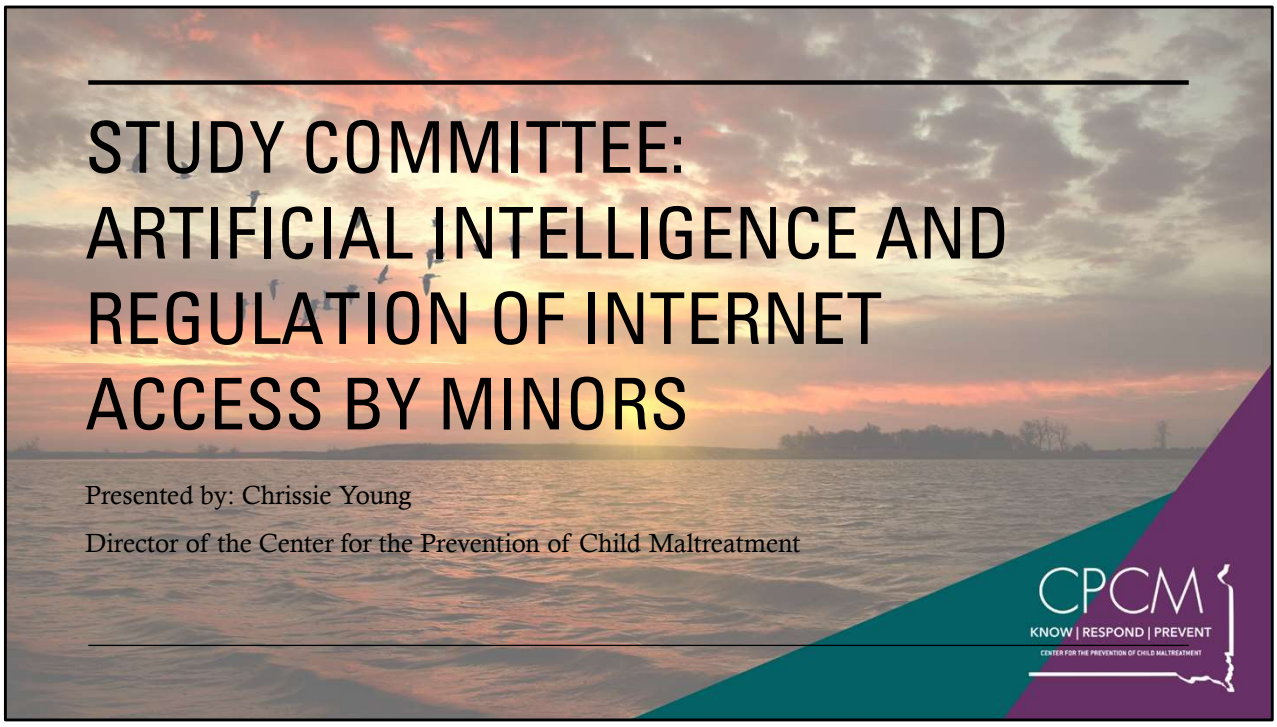
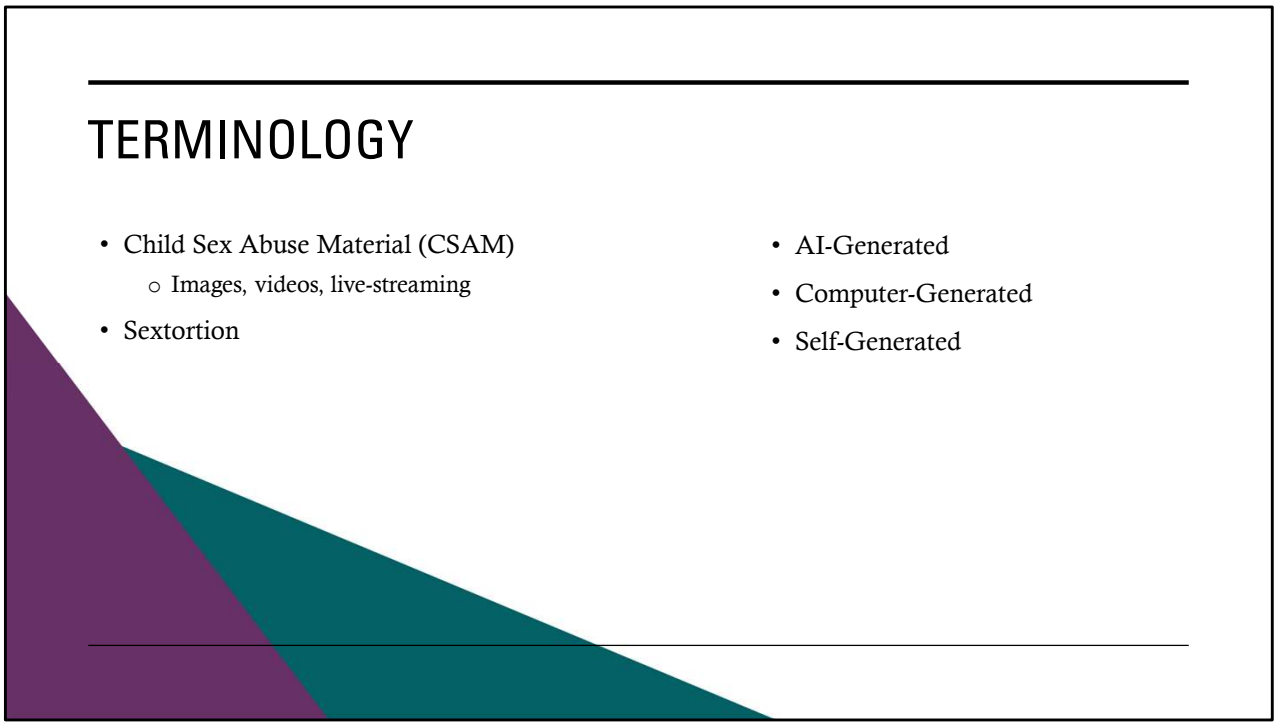

STUDY COMMITTEE:
ARTIFICIAL INTELLIGENCE AND REGULATION OF INTERNET ACCESS BY MINORS
Presented by: Chrissie Young
Director of the Center for the Prevention of Child Maltreatment
CPCM
KNOW | RESPOND | PREVENT
CENTER FOR THE PREVENTION OF CHILD MALTREATMENT

AGENDA

- **CPCM**
- **Terminology**
- **Statistics**
- **Public Health Priority**
- **AI & Social Media**
- **What can we do?**
- **What's effective?**
- **Q&A**


KNOW
Evidence Based Best Practices
RESPOND
Early Intervention
Healing
PREVENT
Create Trauma Informed Communities
CPCM MISSION
CPCM is committed to ending child maltreatment in South Dakota by empowering professionals, communities, and the public to know about, respond to, and prevent child abuse and neglect in South Dakota.
CPCM
KNOW | RESPOND | PREVENT
CENTER FOR THE PREVENTION OF CHILD MALTREATMENT



Opportunities for grooming and hyper-sexualization of our children - bad actors are able to contact them, send them CSAM and pornographic material, sextortion.

THE COST OF CHILD SEXUAL ABUSE

- $9.3B Estimated economic burden of child sexual abuse, including costs associated with health care, productivity losses, child welfare, violence and crime, special education, etc.
- $5.4B Estimated annual cost to incarcerate US adults convicted of sex crimes against children.
- $2M U.S. government funding allocated for child sexual abuse prevention research in 2022.

Letourneau, E. J., Roberts, T. W. M., Malone, L., & Sun, Y. (2023). No Check We Won't Write: A Report on the High Cost of Sex Offender Incarceration. Sexual Abuse, 35(1), 54-82. https://doi.org/10.1177/10790632221078305
Letourneau EJ, Brown DS, Fang X, Hassan A, Mercy JA. The economic burden of child sexual abuse in the United States. Child Abuse Negl. 2018 May;79:413-422. doi: 10.1016/j.chiabu.2018.02.020. Epub 2018 Mar 20. PMID: 29533869; PMCID: PMC6542279.

A GROWING PROBLEM

- Online Predation: Researchers have observed a **threefold increase in self-generated imagery depicting 7–10-year-olds**, as they were increasingly targeted and groomed by internet predators on an industrial scale.
- Children are being targeted and exploited at increasingly younger ages.
  - According to the Canadian Centre for Child Protection, a staggering **78% of the CSAM images and videos assessed were under age 12 and 63% were under age 8**.

End OSEAC. (2024). *Ending OSEAC OMB FY25 request letter*. Retrieved from https://endoseac.org/wp-content/uploads/2024/01/Ending-OSEAC-OMB-FY25-Request-Letter.docx-1.pdf
Thorn. (2024). *Thorn safety by design for generative AI*. Retrieved from https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf

Increase in Prosecution: The number of child sexual abuse material (CSAM) producers sentenced between 2005 and 2019 **increased by 422%** during that time.

A GROWING PROBLEM

- CSAM: In 2022, The National Center for Missing & Exploited Children (NCMEC) received more than 31.9 million reports of suspected child sexual abuse materials, representing over **88.3 million images, videos, and other files**. In 2023, there were over **100 million** such files.
- Online Abuse: There has been a **600% increase** globally in the number of human trafficking cases that were perpetrated using the internet from 2007 to 2018

End OSEAC. (2024). *Ending OSEAC OMB FY25 request letter*. Retrieved from https://endoseac.org/wp-content/uploads/2024/01/Ending-OSEAC-OMB-FY25-Request-Letter.docx-1.pdf

US STUDY BY COMMON SENSE MEDIA

- 12 years old is the average age of pornography exposure online
- 15% reported seeing pornography at an age younger than 10
- 58% of youth reported they accessed pornography online by accident (algorithms, suggested content online)
- >50% said they have viewed violent porn

Michael Robb & Supreet Mann, Teens and pornography, Common Sense Media (2022), https://www.commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf.

PUBLIC HEALTH PRIORITY

- Exposure to CSAM at an early age can be defined as an Adverse Childhood Experience (ACE), with far-reaching negative and harmful impact on well-being and development.
- When children begin viewing even legal, adult pornography at a young age, they begin to consume more extreme material over time as they become desensitized.
- The brain is not fully developed until around the age of 25; more easily impacted/affected by traumatic images.
- Victims of CSAM may experience ongoing trauma because the recordings of their abuse have the potential to be endlessly viewed and shared by those with a sexual interest in children.

Insoll, Tegan, et al. (2021) CSAM Users in the Dark Web: Protecting Children Through Prevention. Suojellaan Lapsia ry. ReDirection Survey Report.

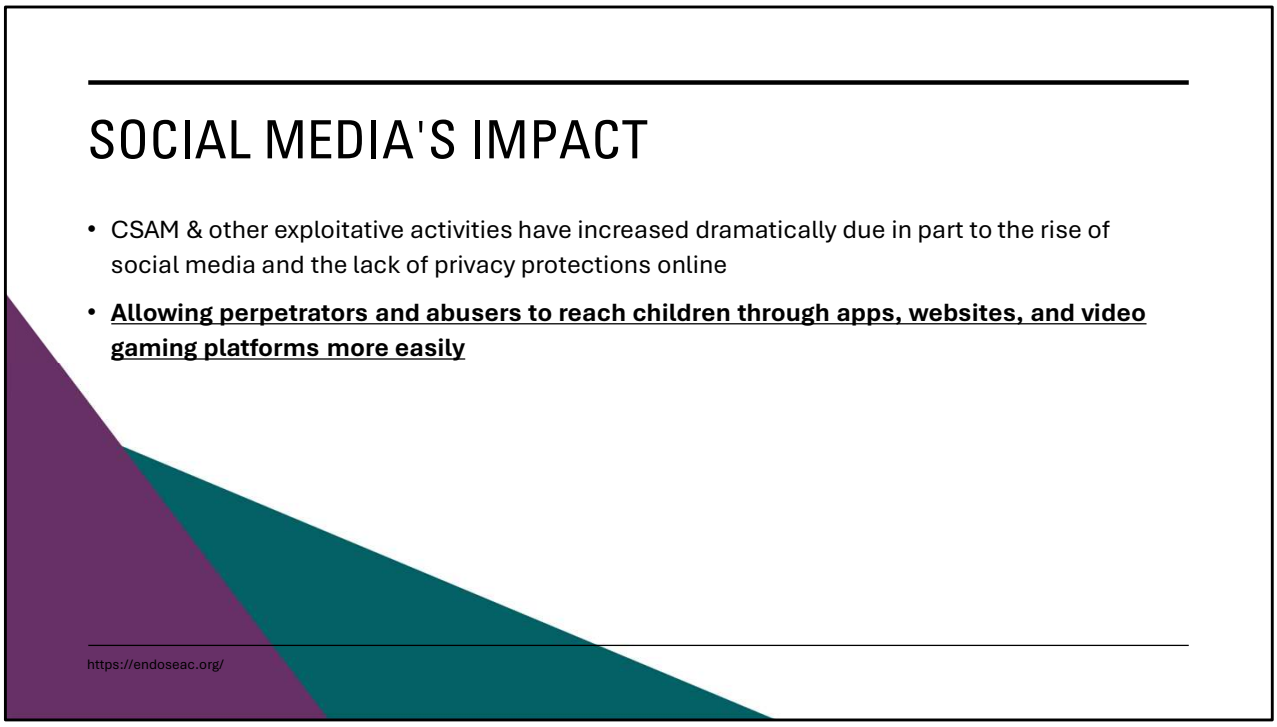


A needle in the haystack problem for law enforcement: sifting through huge amounts of content to find the child in active harm's way. The expanding prevalence of AIG-CSAM is growing that haystack even further, making victim identification more difficult. Hard to know which are real victims in danger, and which are not.

Bad actors collaborate to make these images match the exact likeness of a particular child, but produce new poses, acts and egregious content like sexual violence. These images depict both identified and unidentified survivors of child sexual abuse. Use these in bullying and sextortion.

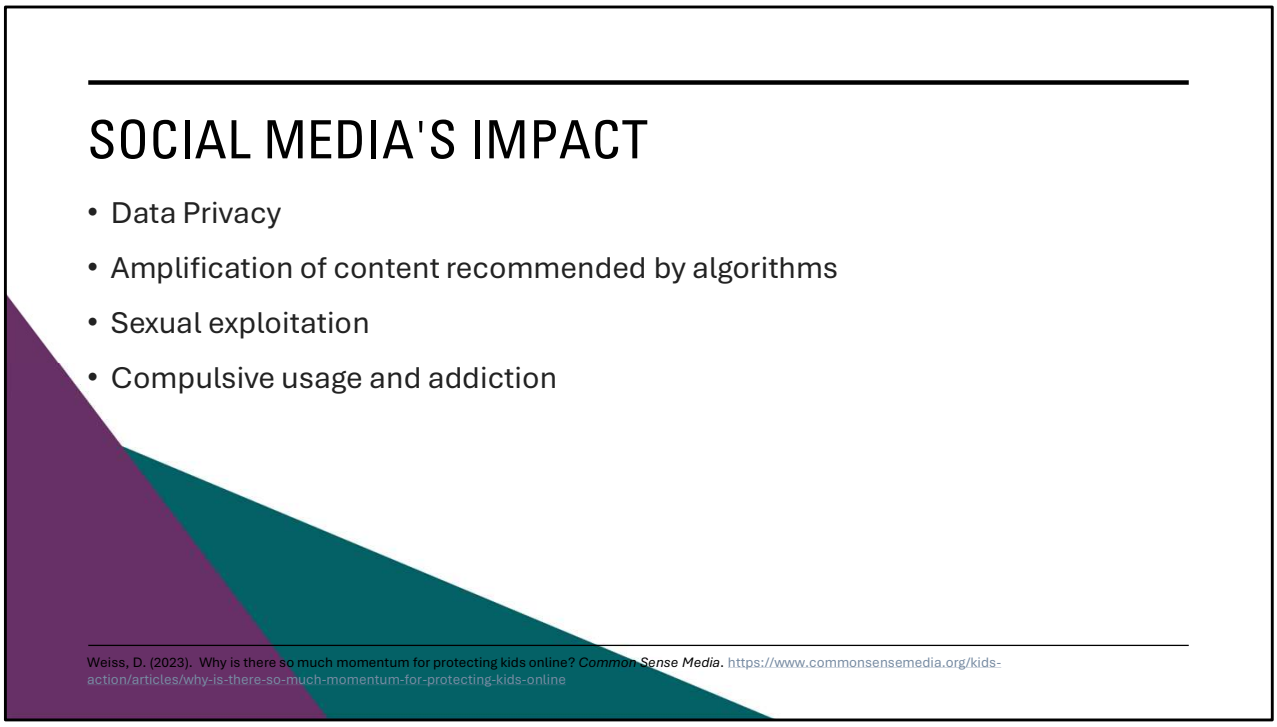
The ease of creating AIG-CSAM, and the ability to do so without the victim's involvement or knowledge, may perpetuate the misconception of this content being "harmless". Research suggests bad actors viewing CSAM may have their fantasies reinforced by viewing abuse imagery and may be at a heightened risk for committing hands on acts of abuse.

AI can support bad actors by providing instruction for hands-on sexual abuse of a child, information on coercive control, details on destroying evidence, and advice on ensuring victims don't disclose.



The more recent rise in Online Sexual Exploitation and Abuse of Children (OSEAC) can also be attributed to the COVID-19 pandemic, which created a perfect storm that increased children's risk. The world shifted to an online environment with teleworking and remote learning. Unfortunately, predators leveraged this as an opportunity to further target children. More children, and much younger children were spending much more time online, on devices, unsupervised than previous to the pandemic. Kids spent their whole day online for school, while parents had to work, so little to no supervision while online.

The areas of online harm spans smartphones, gaming consoles, social media accounts, email and any other medium of contact.

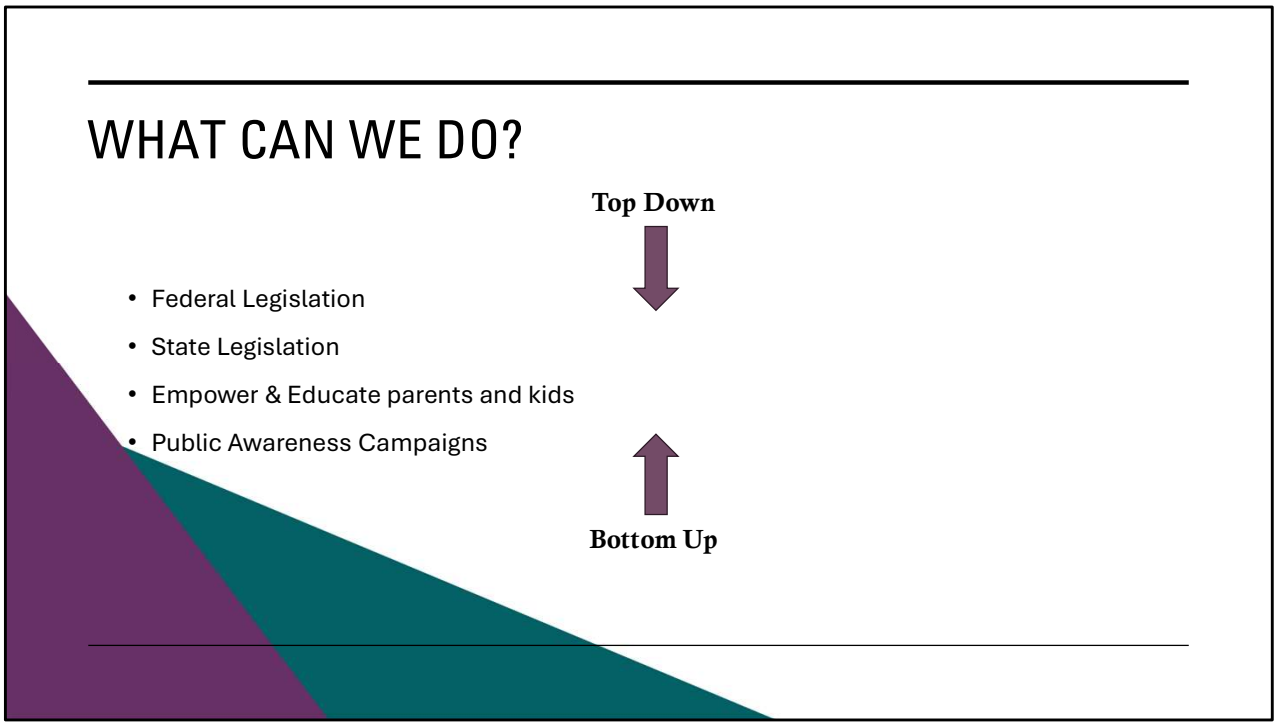


A Mozilla study on regretted YouTube experiences found that most unwanted content was surfaced by the platform's recommendations rather than from user choice. Recommendation algorithms are largely optimized for engagement, which tends to be dominated by small groups of relatively abusive users.

- **Privacy harms:** By the time a child is 13 years old, adtech firms have gathered at least 72 million data points on them, which they can use to manipulate them, such as through targeted ads, or sell to third parties. (Data Privacy for Minors)
- **Amplification of content recommended by algorithms**: Algorithms often take users down dark rabbit holes that recommend content promoting eating disorders, suicidal ideation and self-harm, and dangerous physical challenges like the blackout challenge that are damaging to mental and physical health.
- **Sexual exploitation:** An alarming number of minors have reported sexual encounters with adults online, and many have been coerced into producing child sexual abuse material.

- **Promotion of unhealthy habits**: When kids and teens are targeted with online ads for unhealthy food and drinks, they consume more of these products. Advertising also exposes them to smoking, vaping, drinking, and gambling.
- **Compulsive usage and addiction:** Companies use manipulative design features like endless scroll, autoplay, and push notifications to glue young users to the screen.

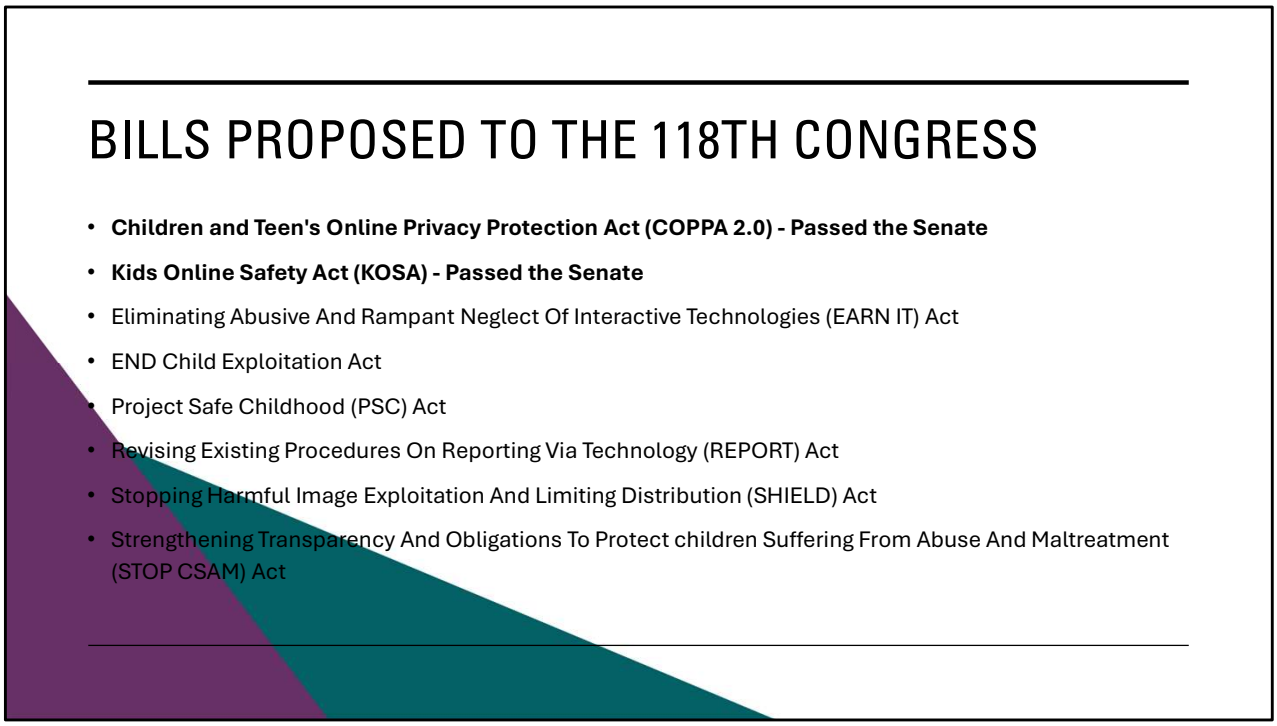
WHAT CAN WE DO?



State's consider laws to limit minor's access to pornographic materials

State's consider laws to enforce default privacy and use setting

State's implement stronger laws against perpetrators



Children and Teens' Online Privacy Protection Act (COPPA 2.0) bans online companies from collecting personal information from users under 17 years old without their consent. It bans targeted advertising to children and teens and creates an eraser button for parents and kids to eliminate personal information online.

Kids Online Safety Act (KOSA)
KOSA requires covered platforms to act in the best interest of children using their services, including mitigating harms they may experience. These platforms would be required to provide child safeguards and tools to children, parents and caregivers, disclose details about their recommendation systems and targeted advertising, improve reporting from parents, children and schools and refrain from facilitating the advertisement of age-restricted products. It also requires platforms to submit annual reports that assess potential risks to children on their platforms.

Eliminating Abusive And Rampant Neglect Of Interactive Technologies (EARN IT) Act
The EARN IT Act revises the federal framework governing the prevention of online sexual exploitation of children. It establishes the National Commission on Online Child Sexual Exploitation Prevention, which will develop best practices for online service providers to prevent, reduce, and respond to the online sexual exploitation of children (provision not included in the House version). The bill creates targeted exceptions to Section 230 of the

Communications Decency Act of 1996 to remove blanket immunity from civil and criminal liability under child sexual abuse material laws. It also creates new reporting requirements to the National Center for Missing and Exploited children (NCMEC)'s CyberTipline. It replaces references of "child pornography" in federal statutes to the more appropriate "child sexual abuse material."

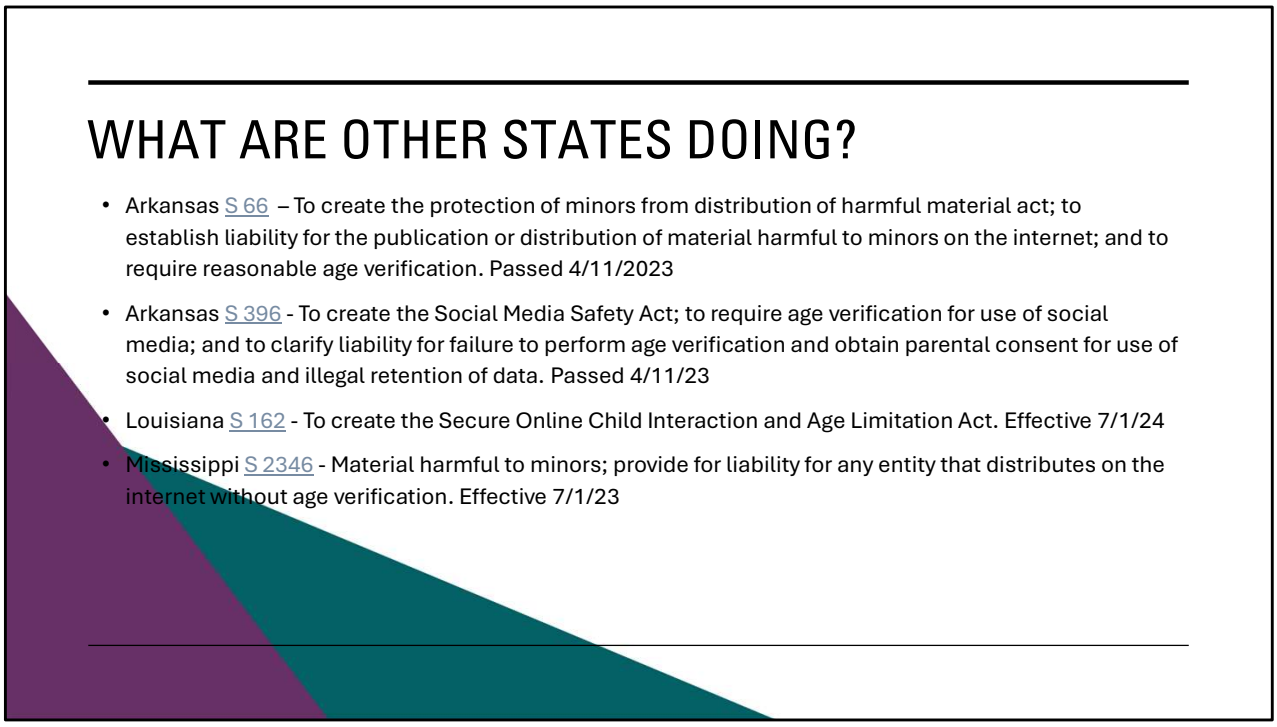
END Child Exploitation Act
This bill increases the length of time online service providers must preserve the contents of the reports submitted to the National Center for Missing and Exploited Children (NCMEC)'s CyberTipline from 90 days to 1 year.

Project Safe Childhood (PSC) Act
This bill modernizes the investigation and prosecution of online child exploitation crimes. It would require federal prosecutors to coordinate with law enforcement and experts to develop training materials and strategies to rescue child victims while quickly arresting offenders. PSC would fund an additional 20 dedicated federal prosecutors at the Department of Justice and clarifies federal laws to close loopholes regarding the production of child sexual abuse materials.

Revising Existing Procedures On Reporting Via Technology (REPORT) Act
The bill would require websites and social media platforms to report violations of federal crimes involving child sex trafficking (e.g. ads selling children for sex) and online enticement or coercion of children; increase the fine (up to $850,000) for websites and social media platforms that knowingly and willfully fail to report child sexual abuse material and online child sexual exploitation; and increase the time that websites and social media platforms are required to preserve evidence for reports that they submit to the CyberTipline, giving law enforcement more time to investigate and prosecute.

Stopping Harmful Image Exploitation And Limiting Distribution (SHIELD) Act
The SHIELD Act ensures that federal prosecutors have appropriate and effective tools to address serious privacy violations by establishing federal criminal liability for individuals who share private, sexually explicit or nude images without consent. It would fill in gaps in existing law that prevent prosecutors from holding those who share explicit images of children accountable and protect the victims of these serious privacy violations, while leaving room for sharing consensual images and images of public concerns.

Strengthening Transparency And Obligations To Protect children Suffering From Abuse And Maltreatment (STOP CSAM) Act
The STOP CSAM Act supports victims and increases accountability and transparency for online platforms. The bill expands protections for child victims and witnesses in federal court; facilitates restitution for victims of child exploitation, human trafficking, sexual assault, and crimes of violence; and empowers victims by making it easier for them to ask technology companies to remove child sexual abuse material and related imagery from their platforms and creating an administrative penalty for failure to comply with removal request.



Thirty-five states and Puerto Rico addressed legislation in 2023, and 12 states enacted bills or adopted resolutions.

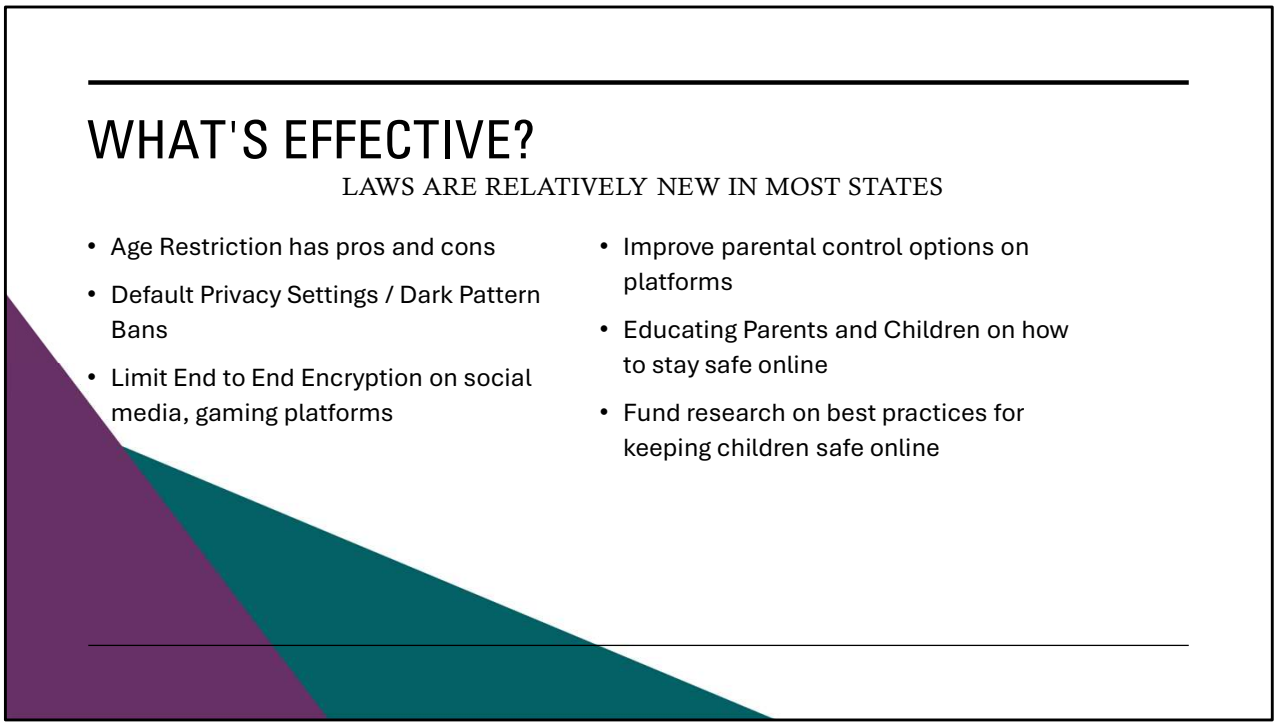
Arkansas S 396 also requires that the company cannot keep/store the information provided to confirm age... If a commercial entity or third party vendor performs a reasonable age verification, the commercial entity shall not retain any identifying information of the individual after access to the material has been granted.

Louisiana S 162: (1) Adults from direct messaging a Louisiana minor account holder unless the minor is already connected to the adult on the service. (2) The display of any advertising in the account based on the Louisiana minor account holder's personal information, except age and location. (3) The collection or use of personal information from the posts, content, messages, text, or usage activities of the account other than information beyond what is adequate, relevant, and reasonably necessary in relation to the purposes for which such information is collected, as disclosed. §1754. Parental access to social media account settings; parental supervision A social media company shall provide a parent or guardian who has given parental consent for a Louisiana minor account holder as provided in this Chapter with a means for the minor account holder or the parent or guardian to initiate account supervision. Such supervision shall include the ability for the parent to view privacy settings of the minor's account, set daily time limits for the

service, schedule breaks, and offer the minor the option to set up parental notifications when the minor reports a person or issue.

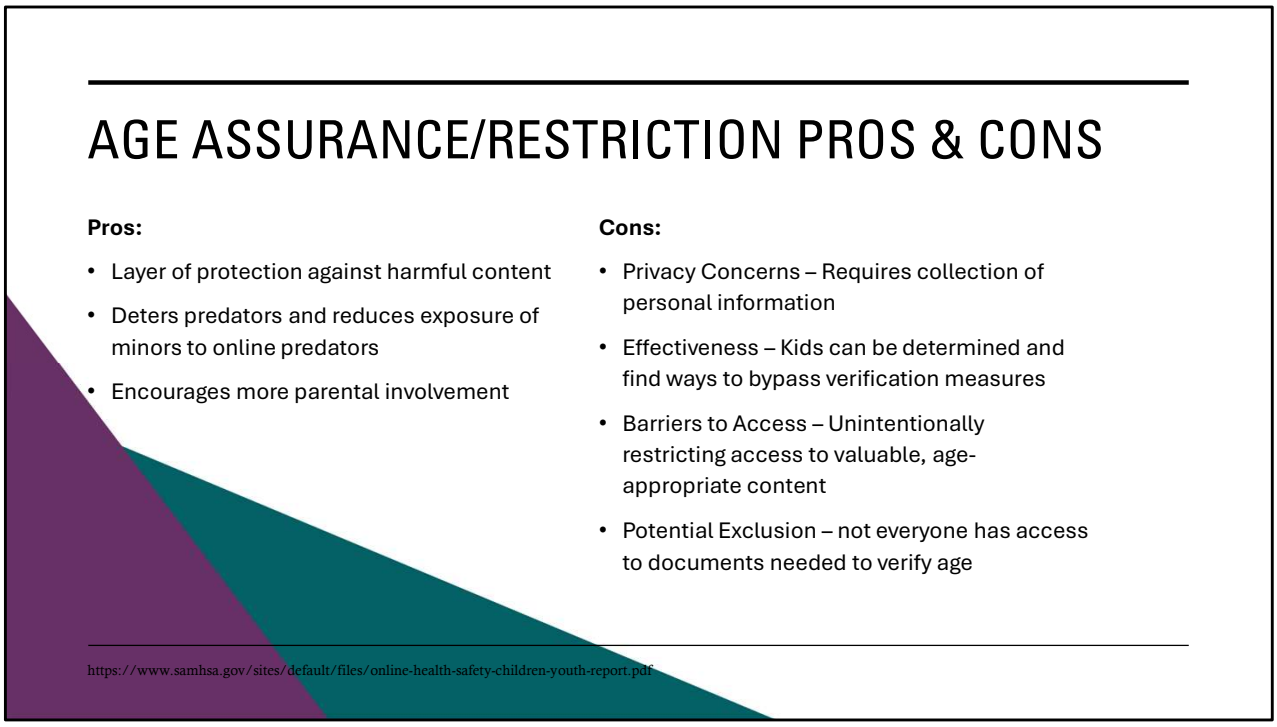
WHAT ARE OTHER STATES DOING?

- Montana S 544 - Revise internet laws related to material harmful to minors; providing for liability for the publishing or distributing of material harmful to minors on the internet; providing for reasonable age verification; providing for individual rights of action; attorney fees; court costs; and punitive damages; providing for exceptions.... Effective 1/1/24
- Texas HB 1181 - Restricting access to sexual material harmful to minors on an internet website. Effective 9/1/23
- Utah SB 152 - Provisions related to the regulation of social media companies and social media platforms. Effective 12/31/23
- Utah SB 287 - To create obligations and liabilities for a commercial entity that provides pornography or other materials harmful to minors. Effective 5/23/23



Age Assurance Details: https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/3-age-assurance-methods/ https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

A safer platform ecosystem would reduce the risk of untrusted actors contacting large numbers of strangers, requiring a positive explicit feedback history (reputation) from a broad set of other users before allowing users to affect people they do not already know. https://www.ag.state.mn.us/Office/Reports/EmergingTechnology.pdf



Many age assurance techniques raise concerns regarding accuracy (e.g., falsifying age or birthdate), privacy (e.g., from documentation, biometric data, or data from other sources), and equity.

Research has found that relying on self-certification alone is not an accurate method for ascertaining age.

Each mechanism discussed above comes with trade-offs—from the burden of complying in an often otherwise frictionless ecosystem, to potentially deterring users of the service to invasion of privacy.

Some methods being used and explored include photo identification matching, facial age estimation, mobile operator network age verification (parents purchasing phones set for an age), and credentials for digital wallets and credit cards.

DEFAULT PRIVACY & USER SETTINGS

Ban "Dark Patterns" Within Platform Design

- Ban Design Features (e.g. optimizing for time spent, infinite scroll, auto-play, aggressive notifications) That Encourage Greater Usage for Children.
- Mandate Aggressive Privacy Defaults to Limit the Unwanted Sharing of Data and Images, Especially for Sexual Content
- Limit the Ability for Small Groups of Users to Manipulate Others

https://www.ag.state.mn.us/Office/Reports/EmergingTechnology.pdf

Dark Patterns refer to the designs of user interfaces and algorithms in ways that benefit the company at the expense of users, often in ways that are imperceptible to the users and are manipulative given that customers would make different choices if given enough information. Focusing more on the design of products minimizes first amendment arguments.

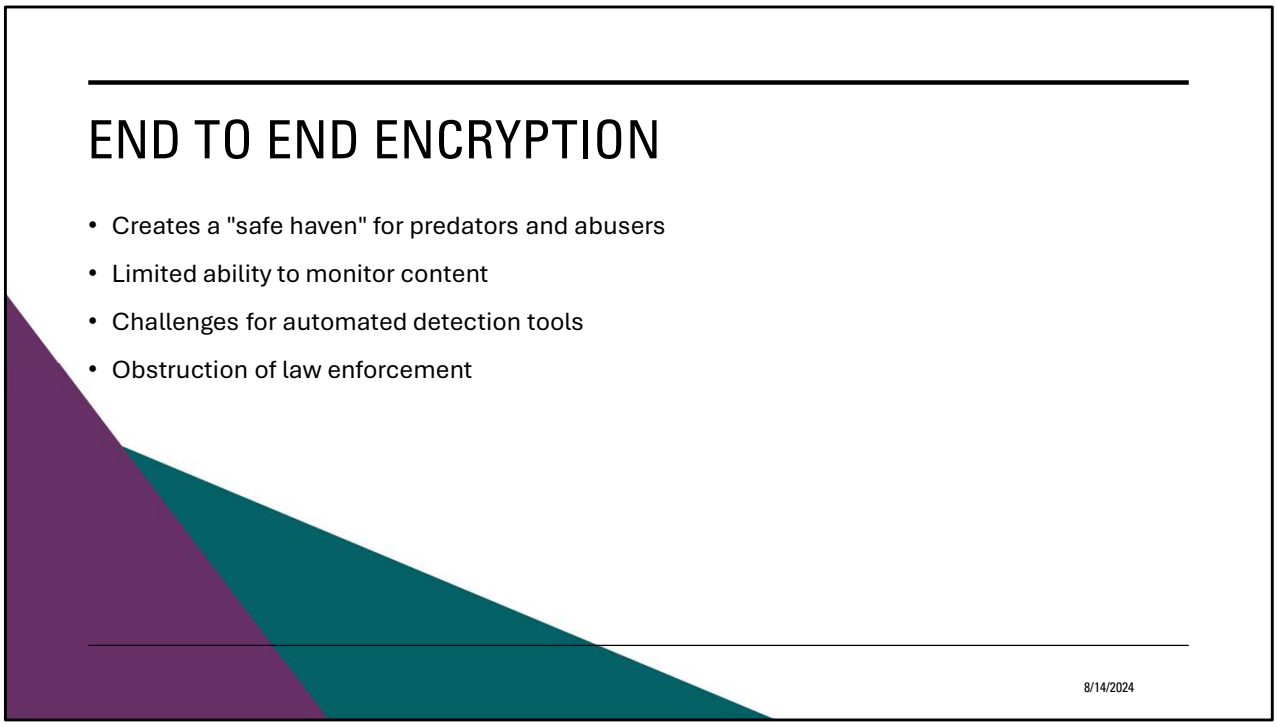
Minors should not be able to receive direct messages from non-followers
Minors cannot add followers, without parental consent.
Auto set to private when they sign up for an account.

DEFAULT PRIVACY & USER SETTINGS

- Mandate Transparency of Product Experimentation That Can Illuminate New Harmful Dark Patterns
- Mandate User and Parent Empowerment via Consumer-Friendly Device-Based Defaults
- Track Technology Platform Specific Impact on User Experience

https://www.ag.state.mn.us/Office/Reports/EmergingTechnology.pdf

8/14/2024



Predators feel more secure in sharing and engaging in child sexual abuse activities.
Makes it extremely difficult for platforms, law enforcement, or other authorities to detect and intercept harmful content, such as child sexual abuse material (CSAM).
E2E encryption can hinder investigations by making it challenging for law enforcement to gather evidence or trace communication related to child sexual abuse. Even with a warrant, authorities may be unable to access the content of communications if they are encrypted.
Platforms often rely on automated tools, such as algorithms and machine learning, to scan for and flag potentially abusive content. These tools cannot function with E2E Encryption.



Toby Russell – Director of South Dakota ICAC – We will not educate ourselves out of this problem. Requires legislative action as well. Prevention and Enforcement.

Parental Controls are often an afterthought; and kids often figure out ways around them. So it's both, and. Tech companies need to do their part to make it functional and easy to figure out, default settings for youth accounts, etc.

CONCLUSION

Several potential opportunities but requires a layered approach.

- **Age restrictions**
- **Default privacy settings / dark pattern bans**
- **Limit End to End Encryption**
- **Improve parental control options**
- **Funding to educate parents and children**
- **Funding research on best practices for keeping children safe online**



8/14/2024


QUESTION & ANSWER
Contact Information
Chrissie Young
Director, CPCM
https://sdcpcm.com/news/end-online-child-abuse/
Christina.Young@usd.edu
712-490-8224
CPCM
KNOW | RESPOND | PREVENT
CENTER FOR THE PREVENTION OF CHILD MALTREATMENT