Initiative 2025-2026 #133
Child Digital Safety

Received by Legislative Council Staff
8/6/2025 at 8:51 am

Colorado Child Safety & Digital Protection Act of 2026

Ballot Title

Shall there be a change to the Colorado Revised Statutes concerning the protection of minors from sexual exploitation in the digital age, and, in connection therewith, criminalizing artificial intelligence–generated and deepfake child sexual abuse material; enhancing penalties for online grooming and sextortion; requiring digital platforms to implement child safety measures including age verification, account transparency, device-based account limits, encryption, screenshot alerts, and geo-masking; authorizing civil remedies for victims; and creating a Digital Child Safety Fund to support enforcement?

Legislative Declaration

The people of Colorado find and declare that:

1. Children are increasingly targeted for sexual exploitation through emerging technologies including artificial intelligence, deepfakes, social media, and digital communications.
2. Existing Colorado law does not fully address AI-generated sexual material, deepfake exploitation, or advanced online grooming and sextortion schemes.
3. Digital platforms operating in Colorado must adopt child safety measures that reflect current and emerging technological threats.
4. This Act establishes criminal, civil, and enforcement provisions necessary to protect minors from sexual exploitation in the digital age.

Section 1 – Definitions

- Minor: A person under eighteen years of age.
- AI-Generated Child Sexual Abuse Material (AI-CSAM): Any visual, audio, or multimedia depiction of a minor in sexual conduct, created or altered by artificial intelligence, machine learning, or digital rendering, whether or not an actual minor was involved.
- Deepfake: Any synthetic or altered media that realistically depicts a minor engaged in sexual conduct.
- Digital Platform: Any online service, application, or software that enables the creation, sharing, or transmission of user-generated content.

Section 2 – Criminal Offenses

1. AI-CSAM – Creation, possession, or distribution is a Class 3 felony, elevated to Class 2 for repeat or large-scale offenses.

2. Deepfake Exploitation – Creation or distribution of nonconsensual sexual deepfake imagery involving a minor is a Class 4 felony, elevated to Class 3 for aggravated uses (e.g., blackmail).
3. Online Grooming & Sextortion – Defined as separate Class 4 felonies, prosecutable regardless of physical contact.

Section 3 – Platform Safety Requirements

Platforms operating in Colorado must implement the following:

1. Age Verification & Parental Consent – For all minor accounts.
2. Account Transparency – Display country of origin, account creation date, and linked account notice in all initial contacts.
3. Device Account Limits & Bans – Limit to five accounts per device in a rolling 30-day period; ban devices used for prohibited conduct for 10 years.
4. Privacy Controls – End-to-end encryption for messaging; screenshot alerts and blocking options; geo-masking to restrict contact by region or country.
5. Takedown Requirement – Remove reported exploitative content within 24 hours.

Section 4 – Civil Remedies

- Victims of AI-CSAM, deepfake exploitation, or sextortion may bring a civil action for actual damages, statutory damages up to $250,000 per violation, attorney's fees, and profits obtained by the offender.
- Platforms that fail to comply with child safety obligations may be liable for civil penalties up to $1,000,000 per violation.

Section 5 – Enforcement & Digital Child Safety Fund

- The Attorney General and District Attorneys shall enforce this Act.
- Civil and criminal penalties shall be deposited into the Digital Child Safety Fund, used exclusively for:
    - ICAC Task Force expansion;
    - Statewide child digital safety education;
    - Community awareness and prevention campaigns.

Section 6 – Severability

If any provision of this Act is held invalid, the remaining provisions remain in effect.