OPPOSE H.R. 7757 – The so-called "Kids Internet and Digital Safety Act"

The American Association for Justice (AAJ) strongly opposes H.R. 7757. This legislation represents a deeply cynical attempt to provide the technology industry with a cleverly veiled way to comprehensively gut stronger state policies, under the guise of child safety. By bundling a limited number of non-controversial research provisions with sweeping giveaways to "Big Tech," the bill seeks to entice bipartisan support while simultaneously dismantling the rights of parents, school districts, and states.

The primary mechanism of this bill is to let *tech companies* define what they are and are not willing to do to protect kids. For example, the KOSA provision of the bill affirmatively says that platforms owe NO duty of care, that the only duty tech companies have is to write their own rules and policies (and as long as they have their own rule, anything that holds them to a different standard is "in conflict" with this bill and thus preempted), **and *throughout the entirety of the bill* actual knowledge is required for both regulation and enforcement, so tech platforms can't be held accountable unless they have *actual knowledge* or *willfully* disregard that a child is on their platforms, while state laws say that tech platforms can be held accountable if they *reasonably should have known* that a child was on their platforms.**

Preemption: The proponents of H.R. 7757 will claim that they saved parents' and school districts' cases, and more protective state laws, because they "fixed" the preemption language throughout the bill with a rule of construction carving out state "trespass, contract, tort, or product liability" law as well as "generally appliable state consumer protections laws". This simply does not fix preemption. **A rule of construction does not save stronger state laws or the cases that are based on them because the majority of primary preemption provisions throughout the bill wipe out state laws that "conflict with" the provisions in the bill.** And many of bill's titles, including the KOSA title, are written to create so many "conflicts" with more protective state laws, that a rule of construction can't save them. The conflict preemption provision will control to wipe out the cases and the state laws. For example, state laws are based on an assumption that a duty of care exists; if you knock out the duty of care via conflict preemption, there is no "tort law" to save—there is no state negligence law if you owe no duty to kids in the first place. Throughout the bill, actual knowledge is required both for regulation and enforcement, so tech platforms can't be held accountable unless they have actual knowledge or willfully disregard that a child is on their platforms, thus coming into conflict with state laws that say that tech platforms can be held accountable if they *reasonably should have known* that a child was on their platforms.

The subsequent analysis addresses H.R. 7757 in its entirety, which serves as a legislative vehicle for several distinct legislative proposals. Specifically, this bill incorporates the Shielding Children from Related Extreme Express Net-content (SCREEN) Act, the Kids Online Safety Act (KOSA), the Safe Messaging for Kids Act, the Stop Profiling Youth (SPY) Kids Act, the Safer Gaming Act, and the Safe Bots Act. Because these bills have been consolidated into a single legislative vehicle, the following analysis examines the cumulative impact of the entire package, highlighting how the collective interaction of these provisions, particularly their overlapping preemption clauses and meaningless "safety" and enforcement standards, creates an unprecedented shield for the technology industry at the expense of children's safety.

Section 2 Definitions

"Know" and "Knows" (Page 5): These terms are defined as having actual knowledge or having acted in willful disregard.

- This is an extremely high standard usually reserved for criminal statutes and requires proving what a tech company subjectively knew about a specific child or group of children, not based on what a company *should have known* given the circumstances.
- Companies only need to provide safeguards for those they "know" are minors, so companies can avoid providing the required safeguards if they don't "know" which accounts belong to minors.

"Personal Information" (Page 6): This is defined as personally identifiable information like first and last names, home addresses, and social security numbers.

- This narrow definition leaves out the exact type of information that social media platforms collect on children to target them. This is information that helps them know what children are feeling, like how long they stay on a video, how fast they swipe, and analytics about the content they are watching.
- It is this type of data, crucially left out of the prohibitions in the bill, that social media companies use to addict children and harm their mental health.

TITLE I: THE SCREEN ACT (Shielding Minors from Obscenity)

Inconsistent Age Verification (Page 10): The bill provides that a user simply "confirming" they are not a minor is insufficient for age verification.

- This higher standard applies only to sexually explicit material. It does not apply to tech companies targeting children within the KOSA sections, meaning confirmation from a social media account that they are not a minor will obviate all other protections in the bill.

Liability Carve-outs (Page 11): While the bill ensures liability for third-party contracts regarding child pornography, it pointedly *fails* to extend similar liability to the other multifaceted harms (self-harm, violence, addiction) addressed in the rest of the bill.

- There is growing awareness, both in the court of public opinion and courts of law, that social media companies are designing platforms to manipulate the developing mind of a child, which cases all types of harm, and yet the bill allows social media to continue without any liability.

Express Preemption (Pages 13 &14): This title wipes out any state law or requirement regarding technology verification measures to prevent minors from accessing sexual material.

- This section restricts states from implementing age-verification measures that exceed federal requirements. While it contains a rule of construction that purports to exempt certain limited categories of law, such as tort and product liability, the breadth of the primary preemption provision threatens to cancel out any laws that are more protective than this Act and does not protect many of the state laws being relied upon to hold tech companies accountable. The carveout for "law of general applicability of a State with respect to consumer protection" is also

meaningless as tech companies can argue that any law that is applied to tech is no longer a law of general applicability.

TITLE II: ADDRESSING HARMS TO MINORS (KOSA PROVISIONS)

Section 201 & Subtitle A: Definitions and Scope

Narrow Age Protections (Page 15): The definition of a "child" is restricted to individuals under 13 years of age.

- This leaves teenagers aged 13 to 17 in a significantly more vulnerable category with fewer protections.

The ADA Definition Loophole (Page 15): The bill defines "compulsive usage" through the lens of the Americans with Disabilities Act (ADA), requiring that usage "limit a major life activity."

- This is a nearly impossible standard to meet in the context of digital addiction and provides a massive loophole for addictive design.

Limiting "User" Definition (Page 16): A "user" is defined strictly as an individual who "registers an account or creates a profile."

- This is an extremely limiting definition that fails to protect children who access platforms without formal registration, such as those using YouTube Kids.

Section 213: Addressing Harms to Minors

Weak Requirements (Page 16): The bill only requires that covered platforms “establish, implement, maintain, and enforce reasonable policies, practices, and procedures that address” certain limited harms to minors.

- The bill does not require companies to make different design choices that will result in less kids getting hurt; all it requires of companies is to have “policies and procedures” that “address” (not decrease) a limited list of harms to kids, but whether they result in actually preventing harm to kids doesn’t matter.

Restricted List of Harms (Page 17): The bill mandates policies for a severely limited list of harms. Most notably, "physical violence" is defined as threats so "severe, pervasive, or objectively offensive" that they impact a "major life activity."

- This definition is so restrictive that it ignores the reality of online harassment and violence and leaves out much of the harm, like suicide, depression, anxiety, and eating disorders, that these platforms are known to cause.
- And again, these are only harms that companies will need policies and procedures to address, which does not meaningfully change anything that they are already doing.

Evisceration of the Duty of Care (Page 18): The rule of construction explicitly states that nothing in this subsection shall be construed to "impose a duty of care on a provider of a covered platform."

- This actively shields platforms from the fundamental legal principle that they owe a duty of care to their young users and their parents, directly conflicting with active litigation nationwide.
- State laws and the cases of parents filed against tech companies are based on an assumption that a duty of care exists; if you knock out the duty of care via conflict preemption, there is no "tort law" to save—there is no negligence case if you owe no duty to kids.

Section 214 & 215: Safeguards and Reporting

The "Actual Knowledge" Barrier (Page 18): Safeguards, parental tools, and default settings only trigger if a provider "knows" a user is a minor.

- This "actual knowledge" standard incentivizes platforms to turn a blind eye and avoid age-verification entirely to escape their safety obligations.

Grandfathering Existing Accounts (Page 21): This section stipulates that if a platform has already provided notice of parental tools before the Act takes effect, and the parent opts out, they are not required to do anything new.

- We all know companies often obtain consent online with long hard to read text boxes with an “I agree” button at the bottom that can be easily missed or clicked through.

Knowing Interference (Page 23): Platforms are only prohibited from "knowingly" using interfaces that impair safety tools.

- The addition of the "knowingly" requirement creates an incredibly difficult evidentiary burden for plaintiffs.

Inadequate Reporting Mechanisms (Page 24): Platforms are required to respond to reports within 10 days unless there is an "imminent threat."

- This undermines CSAM reporting, as platforms may determine that a child who has already been abused is not in "imminent danger," even as the abuse continues to circulate online.

Section 217, 220 & 221: Compliance and Preemption

Outdated Standards (Page 26): Platforms are deemed in compliance with the requirement to provide notice and receive acknowledgement from the parent of someone they know is a minor if they meet the 1998 COPPA standards.

- This 30-year-old standard is wholly inadequate for the modern internet and how social media targets kids and teens.

Targeted Advertising (Page 26): Section 217 explicitly allows targeted advertising to minors as long as it is disclosed as an "ad".

- This is a weak standard that preempts stronger state laws that prohibit profiling children for profit and describes a practice many social media websites like Instagram already do.

Prohibition on Age Verification (Page 31): This section explicitly states that nothing in the subtitle requires age gating or verification functionality.

- This weak standard effectively preempts any state law or judicial ruling that would mandate actual age-verification.

Total Conflict Preemption (Page 31): This section wipes out any state law, rule, or requirement that "conflicts" with this subtitle.

- This language nullifies all stronger state standards, including laws passed through the legislatures and requirements mandated in state courts through the application of common or state law.

SUBTITLE B: SAFE MESSAGING FOR KIDS (PAGE 32)

Limited Coverage (Page 33): This section only applies if the platform "knows" a user is a minor and only covers teens 13 and up.

- Because the bill defines “knows” as actual knowledge or willful disregard, which is an incredibly high standard, this encourages tech companies to turn a blind eye and avoid figuring out if a user is a minor to escape their safety obligations.

FTC Discretion (Page 39): Platforms are only required to take "reasonable measures" to prevent teens from circumventing parental controls.

- The definition of "reasonable" is left to the FTC to define, rather than stronger state laws.

The Encryption "Get Out of Jail Free" Card (Page 40): No requirement may be construed to "compromise the integrity of strong encryption."

- Companies can use this to argue they cannot implement safety or parental controls because it would impact their encryption protocols.

Targeted Hit on Snapchat (Page 41): The effective date is 180 days after enactment.

- This timeline is clearly intended to shut down active litigation and state laws attempting to hold platforms like Snapchat accountable for facilitating predatory contact because the litigation will not be done in 180 days, is directly scrutinizing the ephemeral messaging of the app via state law, and will be preempted by the bill.

SUBTITLE C: STOP PROFILING YOUTH AND KIDS (SPY KIDS ACT)

Account Registration Loophole (Page 41): This subtitle only applies to users who register an account, again ignoring children who access content without a profile.

- By limiting the scope of this subtitle to users who "register an account," this section results in millions of children entirely unprotected. This structural flaw allows platforms to continue harvesting data and targeting content toward children who access sites without an official profile or in “guest” modes.

The "Product Research" Exception (Page 42): Platforms may conduct product-focused research on minors if they claim it is to "improve safety" or "transparency." This allows companies to continue invasive research and data processing under the guise of security.

- The exception for “product research” provides a significant loophole that tech companies will certainly exploit. By allowing invasive data gathering under the vague claims of safety and transparency, this section essentially allows companies to continue the very types of profiling that have already resulted in harm to minors, provided they label it as a security initiative.

Eradication of State Research Protections (Page 42): No state may regulate a platform’s ability to conduct market or product-focused research on a minor, wiping out critical state privacy protections.

- The broad preemption language in Section 244 constitutes a total removal of state authority to oversee how tech companies interact with minors. This provision stops states from passing more protective privacy laws or conducting their own investigations into predatory market research, replacing strong local protections with a weaker federal standard.

TITLE III & IV: SOCIAL GAMING AND AI CHATBOTS

Actual Knowledge Standard for Gaming (Page 44): The "Safer Gaming Act" requires companies to provide safeguards only if they have “actual knowledge” that an account belongs to a minor.

- This incentivizes companies to avoid age-checks, especially since nothing in the bill requires age verification, rendering the entire bill ineffective.

The "Incidental" AI Loophole (Page 49): Companies are exempt from AI regulations if the chat function is "incidental" to the primary service. This allows major platforms to integrate chatbots while arguing they are not "chatbot providers."

- The exemption for AI functions deemed "incidental" to a platform's primary purpose provides a free pass for Big Tech. This vague definition allows major social media and gaming platforms to integrate sophisticated and potentially harmful AI chatbots while legally classifying themselves as non-chatbot providers, effectively insulating themselves and this potentially dangerous tech from federal oversight.

Burden on the Child (Page 49): AI disclosures are only required at the first interaction or if the child prompts the bot to ask if it is an AI. This places the burden of awareness on the minor rather than the developer.

- The bill’s disclosure requirements for AI are fundamentally flawed because it shifts the burden onto a minor to recognize and question whether they are interacting with a bot. By only requiring disclosures at the initial interaction or when the minor requests, this section protects developers and leaves children vulnerable to manipulation by potentially harmful AI systems.

Broad Conflict Preemption (Page 51): Like other titles, these sections include broad preemption clauses designed to nullify any state law that offers more protective standards.

- The inclusion of the expansive preemption clauses in Sections 304 and 407 strips states of their power to pass stronger laws. By nullifying any state law that offers more protection than this weak federal floor, these sections strip parents and state regulators of their ability to hold companies accountable.

TITLE VI: GENERAL PROVISIONS (Enforcement and Immunity Shields)

These provisions apply to the entire Act and serve as the primary mechanism for shielding platforms from meaningful oversight.

Limited Federal and State Enforcement (Page 69): The bill restricts enforcement primarily to the FTC.

- While State Attorneys General (AGs) may enforce the act, they are severely hampered: an AG must provide prior written notice and a complaint to the FTC, which then has an immediate right to intervene. If the FTC or DOJ institutes a civil action, the state action is automatically stayed.

Restricted Judicial Review (Page 73): The bill places extreme limitations on the right to challenge the Act.

- All facial challenges must be brought within 90 days of enactment. Challenges to any specific action or finding under the act must be brought within a mere 60 days, effectively barring most challenges.

Affirmative Encryption Defense (Page 75): This section states that nothing in the act shall be construed to "decrypt or ensure an ability to decrypt" or "preclude the use of any form of encryption, including end-to-end" technology.

- This creates a federal affirmative encryption defense that does not currently exist, since the law cannot be used to ensure decryption, potentially providing a "get out of jail free" card even in Child Sexual Abuse Material (CSAM) cases.

The "Normal Course of Business" Loophole (Page 75): The bill explicitly does not require companies to collect age information if it is not already collected in their normal course of business.

- This incentivizes "willful blindness" to the presence of minors on their platforms.

Effective Date and Preemption (Page 76): Most provisions take effect one year after enactment.

- Any state law in existence or case pending at that time would be subject to immediate preemption, except for very limited carve-outs.