Date: 6/27/2026
Re: Review and Analysis of H.R. 7757, the KIDS Act (as Amended)
Prepared by: Marisa Shea, Legal Fellow at The Tech Oversight Project

The following is a title by title review of the KIDS Act (H.R. 7757), as amended through agreement between Chairman Brett Guthrie and Ranking Member Pallone of the House Energy and Commerce Committee. The analyzed bill text may be found here.

The purported purpose of the bill is to "protect children and teens online, empower parents and strengthen families" - the bill seems to instead combine a variety of proposals without care or understanding for how they may overlap and work together. For example, the bill uses multiple definitions of child, teen, and minor. While it may make sense for Titles to utilize their own definitions, these conflicting designations show an overall lack of cohesion in terms of how to address age appropriate reforms across platform types. Overall, H.R. 7757 seems to offer members their preferred reforms, while ultimately creating a mostly toothless proposal that relies on Big Tech to engage in self regulation through the enactment of "reasonable policies and practices."

The bill has importantly modified its prior preemption language to allow states to enact more protective laws. This was previously included within each applicable Title, but amendments on June 26th instead address preemption for the entire bill within the Title VII - General Provisions. While advocates can appreciate explicitly allowing states to pass more protective laws, those amendments alone should not be reason to enact bad policy that inoculates tech companies against meaningful oversight.

Overarching Definitions

The bill provides a few definitions that apply to the overall Act, with each Title defining additional terms. Some titles redefine the same terms with the same definitions utilized here, this indicates hasty drafting and lack of proper review. The following are defined terms where definitions may raise questions or could be improved upon:

- The bill defines "chatbots" as AI systems that are marketed to and available to consumers with a focus on natural-language communication responses to user inputs. The EPIC People First Chatbot Bill model on the other hand classifies chatbots as any AI, algorithmic, or automated system that generates information. This suggests **the bill's definition of chatbots might be much more narrowly applicable - creating loopholes**.

- The bill defines “design feature” in a manner that only includes what other legislation might consider addictive or high risk features. It only includes features/components that increase use, including: infinite scrolling, autoplay, rewards or incentives for time spent/frequency of use, notifications and push alerts, badges, appearance altering filters, and personalized recommendation systems. **This ignores that all components of a platform are essentially design features - with design choices being decisions that can be made to create safer online platforms vs. more addictive ones**.
- Minors are defined as anyone under the age of 17 - different titles further modify the ages covered.
- Relies on COPPA for its definition of “personal information” - this bill proposes to update that definition to make it more encompassing. It remains **less protective than say the Maryland Online Data Privacy Act**, particularly in regards to derived data and its continued allowance of the sale of minor’s personal information, but is a vast improvement from current COPPA language.
- **Limits “personalized recommendation systems” to those that are fully automated and based on the personal information of the user**; excludes systems that suggests, promotes, or ranks content based on the city/town or age of a user.

Title I: Shielding Minors from Obscenity

Title I is reminiscent of Texas’s age verification law for porn sites. The title applies to websites or other online platforms that are publicly available and that knowingly publish or distribute material on a website or platform where more than one third of the content is “sexual material harmful to minors.” Like the Texas law, Title I has a confusing definition of “sexual material harmful to minors,” to the extent that it is unclear whether the definition would deem some pornographic content suitable for minors.

The bill requires applicable websites and online platforms to institute technology verification measures that prevent those under 18 from accessing the website/platform. The language does not allow companies to utilize self attestation to meet the verification requirements, but does otherwise let companies use commercially available technology to meet the requirements of this Title. There is language suggesting this is not intended to require the use of government identification for verification and limits on the use of personal information collected for verification for any other purposes. However, the Title does not prohibit the use of government IDs for verification and the flexibility provided to website/platforms in terms of choosing a verification method may result in them defaulting to that option. Even the security provisions around technology verification data are rather permissive - allowing the platform, or a contracted third party, to establish, implement and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and availability of the data collected for verification. Given companies current histories of data breaches, what is “reasonable” to the industry might leave much to be desired for consumers.

The title further requires the FTC to consult with “individuals who supply technology verification measure products or have expertise in technology verification measures” in implementing this

title. That suggests the same entities who stand to profit off of age verification products will be consulting with the FTC creating a potential conflict of interest - as they have an incentive to entrench their products as a sort of industry standard.. Given the current corporate capture of this Administration by Big Tech companies, this required seat at the table should alarm advocates more than it might have in the past.

The Title does propose a requirement on the Comptroller General of the US to submit a report to Congress that not only analyzes the effectiveness of the technology verification methods and the compliance of platforms, but also an analysis of the impact of verification on expression, speech, and behavior, among other factors. This would be interesting information, but given this Administration's attacks on government accountability and underfunding of such government entities, it is unclear whether the Comptroller General would have the tools and resources necessary to conduct such an analysis.

Title II: Online Platforms - Subtitle A - Kids Online Safety

All of title II shares a definitions section, it primarily defines "covered platforms." "Covered platforms" are defined as publicly available internet connected websites, software, applications, or electronic services that: enables creation of a username or other identifier that is searchable and can be followed or similarly accessed by other users, has the primary purpose of facilitating the sharing and access to user-generated content, uses a design feature to promote user engagement, and uses personal information of the user to advertise, market, or make content recommendations. This definition would likely not include any chatbots or similar AI products due to the focus on "user-generated content." It also seems to exclude online gaming platforms like Roblox, which seems intentional given Title III. Additionally, the requirement that they use personal information to advertise, market, or make content recommendations and use design features, as limitedly defined by this Act, might offer opportunities for other large platforms to make minor modifications to business practices and then argue they fall out of scope. Given that advertising, marketing, and encouraging user utilization is core to profits, this is hopefully unlikely.

The definitions also define "user" as a registered account holder or someone who creates a profile - thus excluding those who may utilize covered platforms without making accounts. Many of the requirements of the Title are written to apply to both users and visitors of a covered platform, though it is somewhat unclear how some safety settings would be applied without an account. It also defines children as those under 13 and teens as those under 17. The Title's definitions distinguish between direct messaging, ephemeral (or disappearing) messaging, and public/semi-public profiles/feeds. It also provides a confusing definition of "unapproved contact" - stating it means a user of a covered platform with respect to whom another user has not initiated a direct message conversation. This seems to suggest all initial contact would be unapproved - as any initial message would arguably involve two users who had not previously initiated a direct message conversation.

Addressing harms to minors. Title II A requires covered platforms to have and enforce reasonable policies/practices to address the following categories of harm: severe threats of physical violence; sexual exploitation and abuse; distribution, sale, or use of illicit drugs, tobacco products, gambling, or alcohol; and, financial harm caused by deceptive practices. The policies/practices are required to be appropriate to the size and complexity of the platform and to be technically feasible. They are also not allowed to prohibit a minor from independently searching for content or accessing resources related to the enumerated harms. These rules of construction also explicitly prohibit this section from being interpreted as imposing a duty of care on platforms.

It is likely that these provisions would result in no to little change at most major social media platforms. As these companies could likely point to existing policies and procedures tie them back to the provided categories of harm, state the actions they take are what is technically feasible, and suggest they have satisfied this requirement with little cause for recourse given the lack of duty of care and rather subjective requirements. In this way, the bill seems to promise oversight and reform while mostly delivering the status quo.

The Title II A seems to utilize some of the same safety setting requirements we are seeing utilized in state level legislation - it allows minors to hide their online status from other users, block their profile from being recommended to other users, enables the ability to restrict who sends them direct messages, and gives users some control over personalized recommendation systems. For children, the proposal includes parental controls that allow them to change their child's safety settings - while for teens parents are only able to view, rather than control, certain settings. Title II A also prohibits the use of dark patterns to obscure or undermine the use of these safeguards, and further requires the default setting be the most protective for known minors. The safeguards and tools are required to be easily accessible and easy to use.

Title II A seems to allow platforms to be deemed in compliance with notification to parents of the tools/safeguards available and obtaining consent via one consolidated notice for the verifiable consent they're required to obtain under COPPA. This likely will result in a single, lengthy legal disclaimer that many parents will consent to without understanding the information they are handing over or the tools available to them.

Title II A does little to address addictive design features. It doesn't include design changes to address infinite scroll or autoplay - nor does it provide safeguards to allow minors to customize those settings. Rather it gives a broad directive to covered platforms to provide users or visitors with a safeguard against compulsive use. The bill defines compulsive usage based on a cross reference to the ADA - stating it means a persistent and repetitive use of a covered platform that substantially limits a major life activity, as defined in the ADA. This is a standard that would be almost impossible to meet - even for children and teens who feel unable to control their social media usage or who believe their social media use was negatively impacting their overall wellbeing. Given this threshold, covered platforms with have little to do in terms of providing safeguards against design features advocates consider addictive - because it is unlikely they'd meet this required compulsive use threshold. Additionally, the exclusion of AI from the covered

platform definition means this would not apply to Chatbots despite what is beginning to be revealed about their algorithms being designed to encourage overuse.

Furthermore, advocates know there are a variety of design feature changes that can interfere with the addictiveness of these covered platforms - and have seen states take steps to enact such reforms. This suggests the failure to do so in this bill was a policy choice - with lawmakers putting platforms over the wellbeing of kids and teens.

Title II A explicitly states that nothing should be construed as imposing a duty of care of on a covered platform. This combined with a lack of meaningful design changes results in regulation that relies on internal policies and self-enforcement. While some of the safeguards and parental tools may be useful to consumers, there is ample evidence that Big Tech platforms can not be trusted to self-regulate. As a result these provisions continue to fall short in terms of meaningful reform.

Title II: Online Platforms - Subtitle B - Stop Profiling Youth and Kids

Title II B prohibits platforms from conducting market or product research on minors. The provisions carve out research conducted solely to improve privacy, security, transparency, or safety on the covered platforms. This is a seemingly positive provision that would prevent entities like Meta from using young people as their guinea pigs for increased profitization.

However, because of the definition of covered platform, this prohibition would not apply to AI products. Given the state of that industry and its rapid evolution, it is likely that they have or will conduct market or product research on minors. Thus this prohibition applies seemingly only to social media, at a time when several of the large platforms are actually losing users.

Title III: Social Gaming Platforms

At the state level, efforts have been made to require social gaming platforms comply with comprehensive Age Appropriate Design Code Acts or Kids Codes. By separating them into a separate title at the federal level, state lawmakers will be much more likely to carve them out of more comprehensive state level reforms in the future.

By separating online gaming platforms from the requirements of Title III, platforms like Roblox will not be subject to the more design-related safeguards Title II A offers. This ignores how these social gaming platforms use incentives, algorithms, and other design-features akin to social media platforms to target children and teens and expose them to a variety of risks. While the in-game communication safeguards Title III provides likely address some of the risks children and teens face on social gaming platforms and give parents control over those specific means of external communications, they fall far short of the level of protections and reforms needed.

This Title also relies on the term “covered user,” but unlike Title II does not define “user.” It is thus unclear whether the provisions apply only to an account holder/someone who makes a profile or to anyone playing on a social gaming platform.

Title IV: Artificial Intelligence Chatbots

Essentially the only outcome of these provisions are that some chatbots might make incredibly limited disclosures to known minors - which is a far cry from ”safeguarding adolescents from exploitative BOTS.” This Title, like Title III, relies on the term “covered user,” but unlike Title II, does not define “user.” Like in Title III, it is thus unclear whether the provisions apply only to an account holder - such a requirement would be extremely limiting as many Chatbots do not require an account for use.

Title IV also exempts Chatbots that are part of social media platforms or other online products - because it exempts those products with a chatbot function that is incidental to the primary purpose of the website/application/service. Platforms like Instagram or Snap can likely successfully argue that their chatbots are not their services primary purpose and thus avoid even the limited requirements offered here.

The provisions also seem to hint at chatbot personhood. The language specifies that chatbots may not tell the covered user that they are a licensed professional - unless such a statement is true. It is unclear how a chatbot could be a licensed professional and thus unclear how such a statement could be true or why such language is necessary for inclusion.

The required disclosures are extremely limited. The chatbot only has to disclose it is an AI system at the initiation of a first interaction. If a covered user prompts the chatbot as to whether it is AI, the chatbot is supposed to then disclose it is an AI system - but there is no ongoing disclosure requirement. Additionally, any disclosure around crisis resources is only required when the covered user prompts the chatbot about suicide or suicidal ideation. Beyond requirements that the disclosures be in plain language, the Title places no requirements on platforms in regards to how the disclosures appear.

The Title also gives the developers/providers of the Chatbot complete control over policies, practices, and procedures related to both extended use of the chatbot (requiring a note to take a break at the 3 hour mark) and sexual exploitation and abuse, the promotion of gambling, and the promotion of the distribution, sale, or use of illicit drugs, tobacco products, or alcohol. Simply requiring platforms to have policies does little in terms of setting standards or meaningful protections for children and teens.

Title V: Research, Education, and Best Practices for Protecting Minors Online -Subtitle A: Research

Part 1: Safe Social Media Act

This requires the FTC and Secretary of HHS to conduct a study on social media platform use by minors and the potential harms. This seems like something that would make more sense if it was done several years ago. There is a plethora of information available, thanks to whistleblowers and litigation, on what personal information is collected by these companies, how they target children and teens, and how overuse of their platforms impacts young people. It

arguably does not make sense to require such a general study in the same Act targeting specific harm related reforms. Also, this ignores AI and the fact that it is likely the type of tech product currently experiencing the most growth. Yes the bill requires other studies on chatbots, but this seems to be yet another example of policymaking not keeping up with the times.

Part 2: No Fentanyl on Social Media Act
Requires different applicable entities to study and report on the prevalence of and ability for minors to access fentanyl on social media platforms. This seems to address a very specific interest of some members of Congress. It does nothing to require platform accountability or address the underlying issues impacting parents who have lost their children to drug overdoses as result of pills purchased off social media sites.

Part 3: Assessing Safety Tools for Parents and Minors Act
This requires the FTC to work with the industry, parents, and experts to review industry efforts to promote online safety for minors and examine the effectiveness of such efforts. It would likely make more sense to tie this to compliance with the requirements found in other Titles of this Act. But the amalgamation of these various pieces of legislation was done seemingly without an overarching effort to tie the multiple components together.

Part 4: Study on Chatbots and Mental Health of Minors
This study requires the Director of NIH to conduct a 4-year longitudinal study evaluating the risks and benefits of chatbots with respect to the following areas of youth mental health: loneliness, anxiety, social skill building, social isolation, depression, self harm, and suicidal ideation. The idea that the government is studying whether there are benefits to the use of chatbots for dealing with youth social skill building, addressing loneliness, isolation, and anxiety seems rather bleak. It's likely beneficial for this type of research to be available, but there is little direction in the overall framing or requirements. Given the current makeup of HHS and NIH, there is a possibility that the framing could focus more on the benefits than the harms. Additionally, trust in HHS and NIH is seemingly at a low - which may negate the overall usefulness of their mental health research at this time.

<u>Title V: Research, Education, and Best Practices for Protecting Minors Online -Subtitle A: Education</u>

Part 1: Promoting a Safe Internet for Minors Act
This attempt to update the Protecting Children in the 21st Century Act seems to still result in requirements that are antiquated. The provisions do not seem to account for AI or chatbot use, which does seem to ignore the current field. Furthermore, although there's nothing necessarily wrong with trying to teach online literacy in a way that promotes safe internet usage, it continues the narrative that the issue isn't with the platforms or products themselves/their design but rather with their unsafe use.

Part 2: AI Warnings and Resources for Education Act

The focus on benefits of chatbot use within this subsection is alarming. The guise of this subsection is the provision of resources for safe and responsible use - but the resources are being made available approximately 3 years before the study on chatbots and the mental health of minors, required above, is completed. This, and the inclusion of resources on the "benefits" of chatbot use, suggests a predetermined outlook that the FTC should be promoting the use of chatbots by minors. At a time when it is unclear whether there are any chatbot products that present a safe use for minors this framing should be alarming.

Title V: Research, Education, and Best Practices for Protecting Minors Online -Subtitle C: Partnerships and Best Practices

Title V seems to contradict key provisions of other titles. This section requires the creation within 1 year from enactment of a Kids Internet Safety Partnership to weigh in on risks and benefits to minors on online platforms, publish a report on what risks and benefits they've identified, and the efficacy of platform's adopted safeguards and parental tools. Additionally within two years of their establishment, the Partnership is required to publish a playbook for providers and developers of online platforms on widely accepted or evidence based best practices for protections of minors online.

The timelines provided for this contradict with the timelines for reporting requirements under Title V, while seemingly duplicative of some of that work. Additionally, they are being asked to essentially develop recommendations related to safeguards and parental tools that are already being put into effect through other provisions of this Act. Importantly, the Partnership is not being tasked with addressing issues related to AI. This continues the trend of this oversight not recognizing the changing landscape.

Overall, this seems to present a waste of government resources to create a partnership to assess and make recommendations on issues that will arguably be out of date by the time the required playbook is published.

Title VI: Kids Privacy Protections - Subtitle A - COPPA 2.0

As amended, these provisions seem to closely model the Senate version of COPPA 2.0. The updated definition of "personal information" is key to the entirety of this bill, as it all relies on this definition. While COPPA 2.0 greatly improves upon COPPA's existing definition of "personal information" it could be stronger in regards to derived data. Otherwise these provisions expand protections to teens - aged 14 to 17, and give teens the rights to access, correct and delete their data. The KIDS Act version also closes the operator loophole by expanding the definition to cover mobile applications.

A potential issue remains with "verifiable consent." The definition of "verifiable consent" relies on "any reasonable effort" to obtain authorization for the future collection/use/disclosure of a child or teens personal information. This grants a lot of leeway to platforms and weakens efforts for more meaningful consent requirements. Additionally, the KIDS Act carves out Ed Tech from

verifiable consent requirements - this seems to continue a longstanding issue with parents inability to consent to or control the settings of platforms their children interact with in a school setting or on school issued devices. The updates also do nothing to prohibit the sale of children or teens data, but rather maintain the framework allowing such use if overall consent to data use is obtained.

The rules of construction also seem to muddy the interpretation of definitions related to individual-specific advertising. The definition seems to prevent platforms from targeting minors based on personal data relevant to a group of children or teens who have similar attributes, but the rule of construction suggests as long as the advertising is age-appropriate and only the personal information relating to age is utilized, operators may continue to target minors with at least somewhat individualized advertising. A straight ban on individual-specific, or targeted advertising, is an option and it seems to be a choice by policy makers to not have chosen that.

Title VI: Kids Privacy Protections - Subtitle B - Data Broker Disclosures

While a data broker registry seems like a great step forward, the KIDS Act does not present the right approach. To start, it only applies to data brokers that know they are making available a minor's personal data. Bad drafting seems to exempt entities acting as service providers from the (Sec 611(1)(iv) meaning of " covered data broker," while also defining the term "service provider" to include "an entity collecting, processing, or transferring personal data on behalf of and at the direction of an entity acting as a covered data broker (Sec 611(5)(A)(iv))." This seems to create a rather large coverage loophole in an already incredibly small subset of covered data brokers.

Additionally, the inclusion of these provisions in this bill doesn't adequately address the ways data brokers impact everyone's privacy - not just minors. The inclusion negates the idea that federal representatives should be pushing for a ban on the sale of minor's personal information. Rather than requiring disclosure and registry of data brokers trading in minor's personal information, our federal representatives should be pushing for actually meaningful privacy reforms.

Title VII: General Provisions

Like much of this Act, the general provisions are poorly drafted leading to seeming contradictions with other provisions of the Act and potential confusion in regards to implementation and enforcement.

In regards to enforcement, the Act grants the FTC the authority to treat a violation of this Act as a violation of the unfair or deceptive acts or practices under 15 USC 57a(a)(1)(B). The bill seems to continue to limit State Attorneys General enforcement, despite changes to preemption language. The text allows an AG to bring forward a claim, as parens patriae, to seek an enjoinment, enforce compliance, or seek damages. However, Title VII requires a State AG to notify the FTC prior to such action, unless such notice is deemed unfeasible and then they must

provide notice immediately upon filing. The Act also provides the FTC with the right to intervene in a state's case and prohibits a State AG from bringing an action while a federal action is pending. Given this Administration's relationship with the companies this Act seeks to regulate, this seems to present a disadvantage to State AGs - who have been leaders in enforcement against tech companies.

The preemption language has been modified to allow states to enact more protective laws - which should address some State AG's opposition to an earlier version of the law. However, the contradictory drafting and overall loopholes that are created by the KIDS Act suggests some State AGs may continue to have concerns.

On Friday, June 26th, preemption was moved from various titles and instead grouped under Title VII. The preemption language clearly expresses that the bill does not prohibit a State, or their subdivision, from enacting or enforcing any law, rule, requirement, or regulation that provides greater protection to minors than the provisions contained within this bill. The Friday amendments also clarify that the preemption language does not preempt any law, rule, requirement or regulation of a State, or their subdivision, with respect to contract, tort, or product liability. This ensures claims utilizing other areas of state law may continue to proceed.

The contradictions within the rules of construction (Sec. 703) raise questions as to age verification. The language specifies that nothing should be interpreted to require the affirmative collection of any personal information with respect to age that is not already collected in the normal course of business - yet Title 1 clearly requires verification measures to be utilized. Additionally, the bill utilizes a known or should have known standard throughout many other sections which suggests new age information might be collected if an entity wants to apply protections to minors. The bill does not define "know or should have known" and thus it's unclear what might qualify for "should have known." This combined with the language confirming nothing in the bill requires affirmative collection of any personal information with respect to age seems to give companies permission to continue to ignore the age of their users, despite the "known or should have known" standard used throughout the text.