February 25, 2025

House Children & Senior Advocacy Committee
Alabama Legislature
11 South Union Street
Montgomery, AL 36130

Re: HB 317 – "Consumer protection, app store providers and developers required to take certain actions related to age verification and parental consent, Attorney General authorized to bring action for violations as deceptive trade practice, parents authorized to bring civil action" (Oppose)

Dear Chair Shaver and Members of the House Children and Senior Advocacy Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 317 in advance of the Committee hearing on February 26, 2025. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members.

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and parental tools to individually tailor younger users' online use to their developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools allow parents to block specific sites entirely.[2] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.[3]

HB 317's proposed age verification and parental consent requirements for covered app store providers and developers raise significant concerns. The bill risks subjecting businesses to vague compliance requirements and arbitrary enforcement, while jeopardizing consumer privacy. We appreciate the opportunity to expand on these concerns as the Committee considers this proposal.

Requirements under HB 317 are not administrable or well defined, creating serious compliance questions for businesses and users.

HB 317 contains vague definitions that would impose significant requirements and restrictions on app store providers and developers and fail to make children safer. The bill contains overly

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/.
[3] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.

broad knowledge standards that would hold covered entities liable for "knowing or reckless violations," with punitive damages available for "a consistent pattern of knowing or reckless conduct", leaving businesses without any concrete guidelines as to when they might face liability. The bill would also impose burdensome recurring obligations to notify users and obtain "renewed verifiable" consent over any so-called "significant change" to an app's terms of service or privacy policy whenever a modification "[m]aterially changes the app's functionality or user experience[,]" with no objective criteria for businesses to know what constitutes a "material[] change."

Other parts of the bill only appearing once seem to conflate or confuse terms, including text mentioning "obtaining parental disclosure" and "app store developer". Additionally, HB 317 requires but does not appear to explain what it entails for an account to be "affiliated".

Currently available tools to conduct age determination are imperfect in estimating users' ages.

Every approach to age determination presents trade-offs between accuracy and privacy[4]—in addition to significant costs, especially for startups[5]—and there is no one-size-fits-all approach. Different services consider various factors, including but not limited to their user base, the service offered, risk calculation, privacy expectations, and economic feasibility. A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains guiding principles for age assurance and discusses how digital services have used such principles to develop best practices.[6]

The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[7] The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA encourages lawmakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

Age verification and parental consent requirements raise significant privacy concerns.

The proposed bill suggests imposing a government-mandated requirement to verify all Alabama users' ages that conflicts with data minimization principles ingrained in standard

[4] Kate Ruane, *CDT Files Brief in NetChoice v. Bonta Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[5] Engine, *More than just a number: How determining user age impacts startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d51f0b0d4f007b71fe2ba6/1708465932202/Engine+Report+-+More+Than+Just+A+Number.pdf.
[6] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[7] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* Nat'l Inst. of Standards & Tech. (May 30, 2024), https://doi.org/10.6028/NIST.IR.8525.

federal and international privacy and data protection compliance practices.[8] Determining a user's age and verifying parental consent inherently requires collecting additional sensitive data from those users, and any document capable of verifying a user's age will likely contain sensitive information. Requiring companies to collect more user data even as other states require collecting less data places businesses in the untenable position of picking which state laws to comply with, and which to unintentionally violate.[9]

Additionally, verifying age only for operating system and application store users overlooks access to websites via other means. Numerous applications are designed for web browsers, which this method does not cover. While application store age verification might seem like a comprehensive bulwark against certain content deemed undesirable for younger users, in reality, it falls short of achieving that goal.

The Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.[10] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

Furthermore, Section 5's real-time data access requirement would undermine privacy and make children less safe, as developers would have access to sensitive personal information identifying an app store provider's users, including parents of their underage customers.

Age verification and parental consent requirements for online businesses are currently being litigated in several jurisdictions.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.[11] After 25 years, age authentication still remains a vexing technical and social challenge.[12]

Recent state legislation that would implement online parental consent and age verification or estimation measures is currently facing numerous constitutional challenges, and numerous federal judges have placed laws on hold until these challenges can be fully reviewed, including in Arkansas, California, Mississippi, Ohio, Tennessee, Texas, and Utah.[13] CCIA anticipates that

[8] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *see also Principle (c): Data Minimisation*, U.K. Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.
[9] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard.
[10] *Online Age Verification: Balancing Privacy and the Protection of Minors,* CNIL (Sept. 22, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.
[11] *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).
[12] Jackie Snow, *Why age verification is so difficult for websites*, Wall St. J. (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.
[13] *See, e.g.*, *NetChoice v. Bonta*, No. 24-cv-07885, 2025 WL 28610 (N.D. Cal. Jan. 2, 2025); *NetChoice v. Bonta*, No. 22-cv-08861, 2024 WL 5264045 (N.D. Cal. Dec. 31, 2024); *NetChoice, LLC v. Reyes*, No. 23-cv-00911, 2024 WL 4135626 (D. Utah Sept. 10,

forthcoming rulings from the judiciary may be instructive in determining how, or whether, age determination requirements can be tied to granting user access to online speech. CCIA therefore recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated and passing on expensive litigation costs to taxpayers.

* * * * *

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Tom Mann
State Policy Manager, South
Computer & Communications Industry Association

2024); *NetChoice, LLC v. Fitch*, No. 24-cv-00170, 2024 WL 3276409 (S.D. Miss. July 1, 2024); *NetChoice, LLC v. Yost*, 716 F. Supp. 3d 539 (S.D. Ohio 2024); *NetChoice, LLC v. Griffin*, No. 23-cv-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023); *Comput. & Commc'ns Indus. Ass'n et al. v. Paxton*, No. 24-cv-00849, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024).